

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2003-536119

(P2003-536119A)

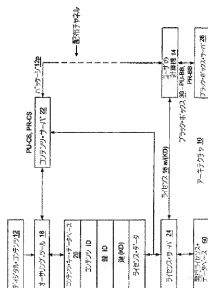
(43) 公表日 平成15年12月2日 (2003.12.2)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 17/60	3 0 2	G 0 6 F 17/60	3 0 2 E 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 Z 5 J 1 0 4
H 0 4 L 9/08		H 0 4 L 9/00	6 7 5 B
9/32			6 7 5 D
			6 0 1 B
審査請求 未請求 予備審査請求 有 (全 101 頁) 最終頁に続く			
(21) 出願番号	特願2000-608539(P2000-608539)	(71) 出願人	マイクロソフト コーポレーション MICROSOFT CORPORATION アメリカ合衆国 ワシントン州 98052- 6399 レッドモンド ワン マイクロソフト ウェイ (番地なし)
(86) (22) 出願日	平成12年2月25日 (2000.2.25)	(72) 発明者	ベイナド, マーカス アメリカ合衆国ワシントン州98007, ペル ビュー, ワンハンドレッドフォーティエ イトス・アベニュー・ノースイースト 5007, ナンバー イー207
(85) 翻訳文提出日	平成13年9月27日 (2001.9.27)	(74) 代理人	弁理士 社本 一夫 (外4名)
(86) 国際出願番号	PCT/US00/04947		
(87) 国際公開番号	WO00/059150		
(87) 国際公開日	平成12年10月5日 (2000.10.5)		
(31) 優先権主張番号	6 0 / 1 2 6, 6 1 4		
(32) 優先日	平成11年3月27日 (1999.3.27)		
(33) 優先権主張国	米国 (US)		
(31) 優先権主張番号	0 9 / 2 9 0, 3 6 3		
(32) 優先日	平成11年4月12日 (1999.4.12)		
(33) 優先権主張国	米国 (US)		

(54) 【発明の名称】 デジタルデジタル権利管理の実施アーキテクチャおよび方法

(57) 【要約】

デジタル権利を実施するための実施アーキテクチャおよび方法を開示する。コンテンツ・サーバからユーザの計算機にデジタル・コンテンツを配信し、ユーザの計算機は受信して、レンダリング・アプリケーションによってデジタル・コンテンツをレンダリングしようとする。レンダリング・アプリケーションは、デジタル権利管理 (DRM) システムを呼び出し、このようなDRMシステムは、計算機に格納されておりデジタル・コンテンツに対応するいずれかのデジタル・ライセンスに基づいて、求められた態様でデジタル・コンテンツをレンダリングする権利が存在するか否かを判定を行なう。権利が存在しない場合、このような権利を与え、デジタル・コンテンツに対応するデジタル・ライセンスを、ライセンス・サーバから要求し、ライセンス・サーバはデジタル・ライセンスをDRMシステムに発行する。計算機は、発行されたデジタル・ライセンスを受信し、受信したデジタル・ライセンスを格納する。



【特許請求の範囲】

【請求項1】 デジタルデジタル権利管理実施アーキテクチャであって、該アーキテクチャが保護対象デジタルデジタル・コンテンツにおける権利を実施し、前記アーキテクチャが、

前記デジタルデジタル・コンテンツを配布するコンテンツ・サーバと、

前記デジタルデジタル・コンテンツに対応し、これとは別個の少なくとも1つのデジタルデジタル・ライセンスを発行するライセンス・サーバと、

前記配布したデジタルデジタル・コンテンツを受信し、当該デジタルデジタル・コンテンツに対応するあらゆるデジタルデジタル・ライセンスを受信しかつ格納する計算機と、

を備え、該計算機が、

前記デジタルデジタル・コンテンツをレンダリングするレンダリング・アプリケーションと、

前記レンダリング・アプリケーションが前記デジタルデジタル・コンテンツをレンダリングしようとするときに、当該レンダリング・アプリケーションが呼び出すデジタルデジタル権利管理(DRM)システムであって、前記計算機に格納されており前記デジタルデジタル・コンテンツに対応するいずれかのデジタルデジタル・ライセンスに基づいて、求められた態様で前記デジタルデジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なう、DRMシステムと、

を有する、デジタルデジタル権利管理実施アーキテクチャ。

【請求項2】 請求項1記載のアーキテクチャにおいて、前記コンテンツ・サーバはネットワークと結合して通信を行い、該ネットワークを通じて前記デジタルデジタル・コンテンツを配布する、アーキテクチャ。

【請求項3】 請求項2記載のアーキテクチャにおいて、前記コンテンツ・サーバはインターネットと結合して通信を行い、インターネットを通じて前記デジタルデジタル・コンテンツを配布する、アーキテクチャ。

【請求項4】 請求項1記載のアーキテクチャにおいて、前記ライセンス・サーバはネットワークと結合して通信を行い、該ネットワークを通じて前記少な

くとも1つのデジタルデジタル・ライセンスを発行する、アーキテクチャ。

【請求項5】 請求項4記載のアーキテクチャにおいて、前記ライセンス・サーバはインターネットと結合して通信を行い、インターネットを通じて前記少なくとも1つのデジタルデジタル・ライセンスを発行する、アーキテクチャ。

【請求項6】 請求項1記載のアーキテクチャにおいて、前記コンテンツ・サーバは携帯メディア・ライターと結合して通信を行い、該携帯メディア・ライターによって書き込んだ可搬媒体上で前記デジタルデジタル・コンテンツを配布し、前記可搬媒体を、光記憶媒体および磁気記憶媒体から成るグループから選択する、アーキテクチャ。

【請求項7】 請求項1記載のアーキテクチャにおいて、前記コンテンツ・サーバは暗号化形態で前記デジタルデジタル・コンテンツを配布する、アーキテクチャ。

【請求項8】 請求項7記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、
前記暗号化デジタルデジタル・コンテンツを解読する解読鍵と、
前記ライセンスによって与えられる権利の記述と、
を含み、前記暗号化デジタルデジタル・コンテンツは、前記ライセンス・サーバからこのようなライセンスを取得せずには、解読およびレンダリングが不可能である、アーキテクチャ。

【請求項9】 請求項8記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、更に、前記ライセンスを前記暗号化デジタルデジタル・コンテンツに結び付けるデジタルデジタル署名を含む、アーキテクチャ。

【請求項10】 請求項1記載のアーキテクチャにおいて、前記DRMシステムが、前記計算機に格納されておりかつ前記デジタルデジタル・コンテンツに対応するいずれのデジタルデジタル・ライセンスに基づいても、求められた態様で前記デジタルデジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、このようなDRMシステムは、計算機のユーザを前記ライセンス・サーバに差し向け、求められた態様でこのようなデジタルデジタル・コンテンツ

をレンダリングするデジタルデジタル・ライセンスを取得させる、アーキテクチャ。

【請求項11】 請求項1記載のアーキテクチャにおいて、前記DRMシステムが、前記計算機に格納されておりかつ前記デジタルデジタル・コンテンツに対応するいずれのデジタルデジタル・ライセンスに基づいても、求められた態様で前記デジタルデジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、このようなDRMシステムは、計算機のユーザ側には何の行為を必要とせずに、前記ライセンス・サーバからデジタルデジタル・ライセンスを透過的に取得する、アーキテクチャ。

【請求項12】 請求項1記載のアーキテクチャにおいて、前記DRMシステムは、デジタルデジタル・ライセンスを格納するライセンス・ストアを含む、アーキテクチャ。

【請求項13】 請求項1記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスをこのようなデジタルデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項14】 請求項13記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスを、公開／秘密鍵技術によって、このようなデジタルデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項15】 請求項1記載のアーキテクチャにおいて、前記ライセンス・サーバは、DRMシステムが前記ライセンスを順守することを当該ライセンス・サーバが信用する場合にのみ、このようなDRMシステムにデジタルデジタル・ライセンスを発行する、アーキテクチャ。

【請求項16】 請求項15記載のアーキテクチャにおいて、前記コンテンツ・サーバは、前記デジタルデジタル・コンテンツを暗号化形態で配布し、前記DRMシステムは、このようなDRMシステムのために解読および暗号化機能を実行する信頼ブラック・ボックスを含む、アーキテクチャ。

【請求項17】 請求項16記載のアーキテクチャにおいて、前記ブラック・ボックスは、前記解読および暗号化機能を実行するために、一意の公開／秘密

鍵対を含む、アーキテクチャ。

【請求項18】 請求項17記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に応答して各デジタルデジタル・ライセンスを発行し、前記ライセンス要求がブラック・ボックス公開鍵を含み、前記ライセンス・サーバは、このようなライセンスの発行に先立って、前記ブラック・ボックス公開鍵にしたがって前記デジタルデジタル・ライセンスの少なくとも一部を暗号化することにより、このようなライセンスをこのようなブラック・ボックスに結び付ける、アーキテクチャ。

【請求項19】 請求項18記載のアーキテクチャにおいて、前記コンテンツ・サーバは前記デジタルデジタル・コンテンツを暗号化形態で配布し、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、前記暗号化デジタルデジタル・コンテンツを解読する解読鍵を含み、前記ライセンス・サーバは、前記ブラック・ボックス公開鍵にしたがって前記ライセンスにおける解読鍵を暗号化する、アーキテクチャ。

【請求項20】 請求項19記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、更に、前記ライセンスによって与えられる権利の記述を含み、前記暗号化デジタルデジタル・コンテンツは、前記ライセンス・サーバからこのようなライセンスを取得しなければ、解読しレンダリングすることが不可能であり、前記ライセンス・サーバは前記解読鍵にしたがって前記ライセンスにおける権利の記述を暗号化する、アーキテクチャ。

【請求項21】 請求項16記載のアーキテクチャにおいて、前記ブラック・ボックスはバージョン番号を含む、アーキテクチャ。

【請求項22】 請求項21記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に応答して各デジタルデジタル・ライセンスを発行し、前記ライセンス要求が前記ブラック・ボックスのバージョン番号を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記ブラック・ボックスのバージョン番号が容認可能か否か判定を行い、前記ライセンス・サーバは、前記ブラック・ボックスのバージョン番号が容

認可できないと判定したとき、前記ブラック・ボックスが更新されるまで、前記ライセンスの発行を拒絶し、前記アーキテクチャは、更に、更新ブラック・ボックスを前記DRMシステムに供給するブラック・ボックス・サーバを備える、アーキテクチャ。

【請求項23】 請求項16記載のアーキテクチャにおいて、前記ブラック・ボックスは、承認された証明機関が供給する証明機関署名を含む、アーキテクチャ。

【請求項24】 請求項23記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に応答して各デジタルデジタル・ライセンスを発行し、前記ライセンス要求が前記証明機関署名を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記証明機関署名が有効か否か判定を行なう、アーキテクチャ。

【請求項25】 請求項15記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、前記ライセンスによって与えられる権利の記述を含み、前記DRMシステムは、前記権利の記述を評価し、レンダリング・アプリケーションによるデジタルデジタル・コンテンツのレンダリングが前記ライセンスの権利の記述に応じたものである場合、このようなレンダリングを許可する、信頼ライセンス評価部を含む、アーキテクチャ。

【請求項26】 請求項1記載のアーキテクチャであって、更に、前記ライセンス・サーバが発行するデジタルデジタル・ライセンスに関する情報を維持する発行ライセンス・データベースを備え、前記計算機が受信したライセンスを紛失した場合、前記発行ライセンス・データベースにおける情報に基づいて、その再発行を可能とした、アーキテクチャ。

【請求項27】 請求項1記載のアーキテクチャであって、更に、前記コンテンツ・サーバが配布する前記デジタルデジタル・コンテンツを、当該アーキテクチャに適した形態でオーサリングするオーサリング・ツールを備える、アーキテクチャ。

【請求項28】 請求項27記載のアーキテクチャにおいて、前記オーサリ

ング・ツールは、解読鍵にしたがって前記デジタルデジタル・コンテンツを暗号化し、前記デジタルデジタル・コンテンツおよび前記暗号化鍵に関する情報をコンテンツ鍵データベースに格納する、アーキテクチャ。

【請求項29】 請求項28記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記デジタルデジタル・コンテンツに対応するライセンスの発行に先立って、前記コンテンツ鍵データベース内にある前記デジタルデジタル・コンテンツおよび前記暗号化鍵に関する情報にアクセスし、このようなライセンスの発行に伴う前記解読鍵を含む、アーキテクチャ。

【請求項30】 デジタルデジタル権利管理の実施方法であって、該方法が保護対象デジタルデジタル・コンテンツにおける権利実施を行い、

コンテンツ・サーバからユーザの計算機に前記デジタルデジタル・コンテンツを配布するステップと、

前記計算機において前記配布されたデジタルデジタル・コンテンツを受信するステップと、

レンダリング・アプリケーションが前記デジタルデジタル・コンテンツのレンダリングを行なおうとするステップと、

このようなレンダリング・アプリケーションが前記デジタルデジタル・コンテンツをレンダリングしようとする際に、前記レンダリング・アプリケーションがデジタルデジタル権利管理(DRM)システムを呼び出すステップと、

前記計算機に格納されており前記デジタルデジタル・コンテンツに対応するいずれかのデジタルデジタル・ライセンスに基づいて、前記DRMシステムが、求められた態様で前記デジタルデジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なうステップと、

前記権利が存在する場合、

このような権利を与え、かつ前記デジタルデジタル・コンテンツに対応しこれとは別個デジタルデジタル・ライセンスを、ライセンス・サーバから要求するステップと、

前記ライセンス・サーバが、前記DRMシステムに前記デジタルデジタル・ライセンスを発行するステップと、

前記計算機が、前記ライセンス・サーバからの前記デジタルデジタル・コンテンツに対応する、前記発行されたデジタルデジタル・ライセンスを受信するステップと、

前記受信したデジタルデジタル・ライセンスを前記計算機上に格納するステップと、
から成る方法。

【請求項31】 請求項30記載の方法において、前記配布するステップは、ネットワークを通じて前記デジタルデジタル・コンテンツを配布するステップから成る、方法。

【請求項32】 請求項31記載の方法において、前記配布するステップは、インターネットを通じて前記デジタルデジタル・コンテンツを配布するステップから成る、方法。

【請求項33】 請求項30記載の方法において、前記発行するステップは、ネットワークを通じて前記デジタルデジタル・ライセンスを発行するステップから成る、方法。

【請求項34】 請求項33記載の方法において、前記発行するステップは、インターネットを通じて前記デジタルデジタル・ライセンスを発行するステップから成る、方法。

【請求項35】 請求項30記載の方法において、前記配布するステップは、光記憶媒体および磁気記憶媒体から成るグループから選択した可搬媒体上で前記デジタルデジタル・コンテンツを配布するステップから成る、方法。

【請求項36】 請求項30記載の方法において、前記配布するステップは、前記デジタルデジタル・コンテンツを暗号化形態で配布するステップから成る、方法。

【請求項37】 請求項36記載の方法であって、更に、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンス毎に、
前記暗号化デジタルデジタル・コンテンツを解読する解読鍵と、
前記ライセンスによって与えられる権利の記述とを含ませるステップを含み、
前記ライセンス・サーバからこのようなライセンスを取得しなければ、前記暗

号化デジタル・コンテンツを解読しレンダリングすることを不可能とした、方法。

【請求項38】 請求項37記載の方法において、前記含ませるステップは、前記デジタル・コンテンツに対応する各ライセンス毎に、前記ライセンスを前記暗号化デジタル・コンテンツに結び付けるデジタル署名を含ませるステップから成る、方法。

【請求項39】 請求項30記載の方法において、前記デジタル・ライセンスを要求するステップは、前記DRMシステムが計算機のユーザを前記ライセンス・サーバに差し向け、求められた態様でこのようなデジタル・コンテンツをレンダリングするデジタル・ライセンスを取得するステップから成る、方法。

【請求項40】 請求項30記載の方法において、前記デジタル・ライセンスを要求するステップは、計算機ユーザの側では何の行為も必要とせずに、前記DRMシステムが、前記ライセンス・サーバからデジタル・ライセンスを透過的に取得するステップから成る、方法。

【請求項41】 請求項30記載の方法において、前記格納するステップは、前記DRMシステムが、受信した前記ライセンス・サーバを前記DRMシステムのライセンス・ストアに格納するステップから成る、方法。

【請求項42】 請求項30記載の方法であって、更に、前記ライセンス・サーバが、前記デジタル・ライセンスを前記対応するデジタル・コンテンツに結び付けるステップを含む、方法。

【請求項43】 請求項42記載の方法であって、公開／秘密鍵技術によって、前記ライセンス・サーバが前記デジタル・ライセンスを前記対応するデジタル・コンテンツに結び付けるステップを含む、方法。

【請求項44】 請求項30記載の方法において、前記発行するステップは、前記DRMシステムが前記ライセンスを順守することを、前記ライセンス・サーバが信用する場合にのみ、前記ライセンス・サーバが前記デジタル・ライセンスをこのようなDRMシステムに発行するステップから成る、方法。

【請求項45】 請求項44記載の方法において、前記配布するステップは、前記コンテンツ・サーバが前記デジタル・コンテンツを暗号化形態で配布する

ステップから成り、更に、前記DRMシステムにおいて信頼ブラック・ボックスを用いて、このようなDRMシステムのために解読および暗号化機能を実行するステップを含む、方法。

【請求項46】 請求項45記載の方法において、前記ブラック・ボックスは公開／秘密鍵対を含み、前記デジタル・ライセンスを要求するステップは、前記要求にブラック・ボックス公開鍵を含ませるステップから成り、更に、このようなライセンスの発行に先立って、前記ブラック・ボックス公開鍵にしたがって前記デジタル・ライセンスの少なくとも一部を前記ライセンス・サーバが暗号化することにより、このようなライセンスをこのようなブラック・ボックスに結び付けるステップを含む、方法。

【請求項47】 請求項46記載の方法において、前記配布するステップは、前記デジタル・コンテンツを暗号化形態で配布するステップから成り、更に、

前記デジタル・コンテンツに対応する各デジタル・ライセンス毎に、前記暗号化デジタル・コンテンツを解読する解読鍵を含ませるステップと、

前記ブラック・ボックス公開鍵にしたがって、前記ライセンス・サーバが前記ライセンス内にある前記解読鍵を暗号化するステップと、
を含む、方法。

【請求項48】 請求項47記載の方法であって、更に、

前記デジタル・コンテンツに対応する各デジタル・ライセンス毎に、前記ライセンスによって与えられる権利の記述を含ませるステップであって、前記ライセンス・サーバからのこのようなライセンスを取得しなければ、前記暗号化デジタル・コンテンツを解読しレンダリングすることを不可能とする、ステップと、

前記解読鍵にしたがって前記ライセンス・サーバが前記ライセンス内の権利の記述を暗号化するステップと、
を含む、方法。

【請求項49】 請求項45記載の方法において、前記ブラック・ボックスはバージョン番号を含み、前記デジタル・ライセンスを要求するステップは、前記ブラック・ボックスのバージョン番号を前記要求内に含ませるステップから成り、更に、

前記ライセンスの発行に先立って、前記ライセンス・サーバが前記ブラック・ボックスのバージョン番号が容認可能か否か判定を行なうステップと、

前記ブラック・ボックスのバージョン番号が容認可能でないと判定したとき、前記ライセンス・サーバが、前記ブラック・ボックスを更新するまで、前記ライセンスの発行を拒絶するステップと、
を含み、前記アーキテクチャが、前記DRMシステムに更新ブラック・ボックスを供給するブラック・ボックス・サーバを備える、方法。

【請求項50】 請求項45記載の方法において、前記ブラック・ボックスは、承認された証明機関が供給する証明機関署名を含み、前記デジタル・ライセンスを要求するステップは、前記証明機関署名を含ませ、前記ライセンスの発行に先立って、前記ライセンス・サーバが前記証明機関署名が有効か否か判定を行なうステップを含む、方法。

【請求項51】 請求項44記載の方法において、前記デジタル・ライセンスを発行するステップは、前記ライセンスによって与えられる権利の記述を前記デジタル・ライセンスに含ませるステップを含み、更に、

前記DRMシステムの信頼ライセンス評価部が、前記権利の記述を評価するステップと、

前記レンダリング・アプリケーションによる前記デジタル・コンテンツのレンダリングが、前記ライセンスの権利の記述に応じたものである場合にのみ、このようなレンダリングを許可するステップと、
を含む、方法。

【請求項52】 請求項30記載の方法であって、更に、前記ライセンス・サーバが発行するデジタル・ライセンスに関する情報を発行ライセンス・データベースに維持するステップを含み、前記計算機が受信したライセンスを紛失した場合、前記発行ライセンス・データベース内にある情報に基づいて、その再発行を可能とする、方法。

【請求項53】 請求項30記載の方法であって、更に、オーサリング・ツールによって、前記コンテンツ・サーバが配布したデジタル・コンテンツを、前記アーキテクチャに適した形態でオーサリングするステップを含む、方法。

【請求項54】 請求項53記載の方法において、前記オーサリングするステップは、

解読鍵にしたがって前記デジタル・コンテンツを暗号化するステップと、
前記デジタル・コンテンツおよび前記暗号化鍵に関する情報を、コンテンツ鍵データベースに格納するステップと、
を含む、方法。

【請求項55】 請求項54記載の方法において、前記デジタル・ライセンスを発行するステップは、

前記デジタル・コンテンツに対応するライセンスの発行に先立って、前記ライセンス・サーバが前記コンテンツ鍵データベース内の前記デジタル・コンテンツおよび前記暗号化鍵に関する情報にアクセスするステップと、

このような発行されたライセンスに、前記解読鍵を含ませるステップと、
を含む、方法。

【請求項56】 デジタル権利管理実施アーキテクチャであって、該アーキテクチャは保護対象デジタル・コンテンツにおける権利を実施し、

ネットワークと通信するように結合され、前記デジタル・コンテンツを前記ネットワークを通じて配布するコンテンツ・サーバと、

前記デジタル・コンテンツに対応しこれとは別個の少なくとも1つのデジタル・ライセンスを発行するライセンス・サーバであって、前記ネットワークと通信するように結合され、前記少なくとも1つのデジタル・ライセンスを前記ネットワークを通じて発行する、ライセンス・サーバと、

前記ネットワークと通信するように結合され、前記配布されたデジタル・コンテンツを受信し、かつ前記デジタル・コンテンツに対応するいずれかのデジタル・ライセンスを受信する計算機と、
から成り、前記計算機が、

前記デジタル・コンテンツに対応するいずれかのデジタル・ライセンスを格納するメモリと、

前記デジタル・コンテンツをレンダリングしようとするレンダリング・アプリケーションと、

前記レンダリング・アプリケーションが前記デジタル・コンテンツをレンダリングしようとするときに、当該レンダリング・アプリケーションが呼び出すデジタル権利管理（DRM）システムであって、前記計算機に格納されており前記デジタル・コンテンツに対応するいずれかのデジタル・ライセンスに基づいて、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なう、DRMシステムと、
を有する、デジタル権利実施アーキテクチャ。

【請求項57】 請求項56記載のアーキテクチャにおいて、前記コンテンツ・サーバはインターネットと結合して通信を行い、インターネットを通じて前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項58】 請求項56記載のアーキテクチャにおいて、前記ライセンス・サーバはインターネットと結合して通信を行い、インターネットを通じて前記少なくとも1つのデジタル・ライセンスを発行する、アーキテクチャ。

【請求項59】 請求項56記載のアーキテクチャにおいて、前記コンテンツ・サーバは携帯メディア・ライタと結合して通信を行い、該携帯メディア・ライタによって書き込んだ可搬媒体上で前記デジタル・コンテンツを配布し、前記可搬媒体を、光記憶媒体および磁気記憶媒体から成るグループから選択し、前記計算機は、前記可搬媒体に対応し、該可搬媒体を受け入れ読み取りを行なう可搬媒体リーダを含む、アーキテクチャ。

【請求項60】 請求項56記載のアーキテクチャにおいて、前記コンテンツ・サーバは暗号化形態で前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項61】 請求項60記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、
前記暗号化デジタル・コンテンツを解読する解読鍵と、
前記ライセンスによって与えられる権利の記述と、
を含み、前記ライセンス・サーバからこのようなライセンスを取得せずには、前記暗号化デジタル・コンテンツを解読しレンダリングすることを不可能とした、
アーキテクチャ。

【請求項62】 請求項61記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、更に、前記ライセンスを前記暗号化デジタル・コンテンツに結び付けるデジタル署名を含む、アーキテクチャ。

【請求項63】 請求項56記載のアーキテクチャにおいて、前記DRMシステムが、前記計算機に格納されておりかつ前記デジタル・コンテンツに対応するいずれのデジタル・ライセンスに基づいても、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、このようなDRMシステムは、計算機のユーザを前記ライセンス・サーバに差し向け、求められた態様でこのようなデジタル・コンテンツをレンダリングするデジタル・ライセンスを取得させる、アーキテクチャ。

【請求項64】 請求項56記載のアーキテクチャにおいて、前記DRMシステムが、前記計算機に格納されておりかつ前記デジタル・コンテンツに対応するいずれのデジタル・ライセンスに基づいても、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、このようなDRMシステムは、計算機のユーザ側には何の行為を必要とせずに、前記ライセンス・サーバからデジタル・ライセンスを透過的に取得する、アーキテクチャ。

【請求項65】 請求項56記載のアーキテクチャにおいて、前記DRMシステムは、デジタル・ライセンスを格納するライセンス・ストアを含む、アーキテクチャ。

【請求項66】 請求項56記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスをこのようなデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項67】 請求項66記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスを、公開／秘密鍵技術によって、このようなデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項68】 請求項56記載のアーキテクチャにおいて、前記ライセンス・サーバは、DRMシステムが前記ライセンスを順守することを当該ライセンス・サーバが信用する場合にのみ、このようなDRMシステムにデジタル・ライ

センスを発行する、アーキテクチャ。

【請求項69】 請求項68記載のアーキテクチャにおいて、前記コンテンツ・サーバは、前記デジタル・コンテンツを暗号化形態で配布し、前記DRMシステムは、このようなDRMシステムのために解読および暗号化機能を実行する信頼ブラック・ボックスを含む、アーキテクチャ。

【請求項70】 請求項69記載のアーキテクチャにおいて、前記ブラック・ボックスは、前記解読および暗号化機能を実行するために、一意の公開／秘密鍵対を含む、アーキテクチャ。

【請求項71】 請求項70記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求がブラック・ボックス公開鍵を含み、前記ライセンス・サーバは、このようなライセンスの発行に先立って、前記ブラック・ボックス公開鍵にしたがって前記デジタル・ライセンスの少なくとも一部を暗号化することにより、このようなライセンスをこのようなブラック・ボックスに結び付ける、アーキテクチャ。

【請求項72】 請求項71記載のアーキテクチャにおいて、前記コンテンツ・サーバは前記デジタル・コンテンツを暗号化形態で配布し、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、前記暗号化デジタル・コンテンツを解読する解読鍵を含み、前記ライセンス・サーバは、前記ブラック・ボックス公開鍵にしたがって前記ライセンスにおける解読鍵を暗号化する、アーキテクチャ。

【請求項73】 請求項72記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、更に、前記ライセンスによって与えられる権利の記述を含み、前記ライセンス・サーバからこのようなライセンスを取得しなければ、前記暗号化デジタル・コンテンツを解読しレンダリングすることが不可能であり、前記ライセンス・サーバは前記解読鍵にしたがって前記ライセンスにおける権利の記述を暗号化する、アーキテクチャ。

【請求項74】 請求項69記載のアーキテクチャにおいて、前記ブラック・ボックスはバージョン番号を含む、アーキテクチャ。

【請求項75】 請求項74記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求が前記ブラック・ボックスのバージョン番号を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記ブラック・ボックスのバージョン番号が容認可能か否か判定を行い、前記ライセンス・サーバは、前記ブラック・ボックスのバージョン番号が容認可能でないと判定したとき、前記ブラック・ボックスが更新されるまで、前記ライセンスの発行を拒絶し、前記アーキテクチャは、更に、更新ブラック・ボックスを前記DRMシステムに供給するブラック・ボックス・サーバを備える、アーキテクチャ。

【請求項76】 請求項69記載のアーキテクチャにおいて、前記ブラック・ボックスは、承認された証明機関によって供給される証明機関署名を含む、アーキテクチャ。

【請求項77】 請求項76記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に응答して各デジタル・ライセンスを発行し、前記ライセンス要求が前記証明機関署名を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記証明機関署名が有効か否か判定を行なう、アーキテクチャ。

【請求項78】 請求項68記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、前記ライセンスによって与えられる権利の記述を含み、前記DRMシステムは、前記権利の記述を評価し、レンダリング・アプリケーションによるデジタル・コンテンツのレンダリングが前記ライセンスの権利の記述に応じたものである場合、このようなレンダリグを許可する、信頼ライセンス評価部を含む、アーキテクチャ。

【請求項79】 請求項56記載のアーキテクチャであって、更に、前記ライセンス・サーバが発行するデジタル・ライセンスに関する情報を維持する発行ライセンス・データベースを備え、前記計算機が受信したライセンスを紛失した場合、前記発行ライセンス・データベースにおける情報に基づいて、その再発行を可能とした、アーキテクチャ。

【請求項80】 請求項56記載のアーキテクチャであって、更に、前記コンテンツ・サーバが配布する前記デジタル・コンテンツを、当該アーキテクチャに適した形態でオーサリングするオーサリング・ツールを備える、アーキテクチャ。

【請求項81】 請求項80記載のアーキテクチャにおいて、前記オーサリング・ツールは、解読鍵にしたがって前記デジタル・コンテンツを暗号化し、前記デジタル・コンテンツおよび前記暗号化鍵に関する情報をコンテンツ鍵データベースに格納する、アーキテクチャ。

【請求項82】 請求項81記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記デジタル・コンテンツに対応するライセンスの発行に先立って、前記コンテンツ鍵データベース内にある前記デジタル・コンテンツおよび前記暗号化鍵に関する情報にアクセスし、このようなライセンスの発行に伴う前記解読鍵を含む、アーキテクチャ。

【請求項83】 デジタル権利管理実施アーキテクチャであって、該アーキテクチャは保護対象デジタル・コンテンツにおける権利を実施し、前記アーキテクチャが、

前記アーキテクチャに適した形態で前記デジタル・コンテンツのオーサリングを行なうオーサリング・ツールと、

前記オーサリング・ツールから前記デジタル・コンテンツを受け取り、該デジタル・コンテンツを配布するコンテンツ・サーバと、

前記デジタル・コンテンツに対応し、これとは別個の少なくとも1つのデジタル・ライセンスを発行するライセンス・サーバであって、計算機が、前記配布したデジタル・コンテンツを受信し、当該デジタル・コンテンツに対応するあらゆるデジタル・ライセンスを受信しかつ格納する、ライセンス・サーバと、
を備え、該計算機が、

前記デジタル・コンテンツをレンダリングするレンダリング・アプリケーションと、

前記レンダリング・アプリケーションが前記デジタル・コンテンツをレンダリングしようとするときに、当該レンダリング・アプリケーションが呼び出すデジ

タル権利管理（DRM）システムであって、前記計算機に格納されており前記デジタル・コンテンツに対応するいずれかのデジタル・ライセンスに基づいて、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なう、DRMシステムと、
を有する、デジタル権利実施アーキテクチャ。

【請求項84】 請求項83記載のアーキテクチャにおいて、前記コンテンツ・サーバはネットワークと結合して通信を行い、該ネットワークを通じて前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項85】 請求項84記載のアーキテクチャにおいて、前記コンテンツ・サーバはインターネットと結合して通信を行い、インターネットを通じて前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項86】 請求項83記載のアーキテクチャにおいて、前記ライセンス・サーバはネットワークと結合して通信を行い、該ネットワークを通じて前記少なくとも1つのデジタル・ライセンスを発行する、アーキテクチャ。

【請求項87】 請求項86記載のアーキテクチャにおいて、前記ライセンス・サーバはインターネットと結合して通信を行い、インターネットを通じて前記少なくとも1つのデジタル・ライセンスを発行する、アーキテクチャ。

【請求項88】 請求項83記載のアーキテクチャにおいて、前記コンテンツ・サーバは携帯メディア・ライタと結合して通信を行い、該携帯メディア・ライタによって書き込んだ可搬媒体上で前記デジタル・コンテンツを配布し、前記可搬媒体を、光記憶媒体および磁気記憶媒体から成るグループから選択する、アーキテクチャ。

【請求項89】 請求項1記載のアーキテクチャにおいて、前記コンテンツ・サーバは暗号化形態で前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項90】 請求項89記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、
前記暗号化デジタル・コンテンツを解読する解読鍵と、
前記ライセンスによって与えられる権利の記述と、

を含み、前記ライセンス・サーバからこのようなライセンスを取得せずには、前記暗号化デジタル・コンテンツを解読しレンダリングすることを不可能とした、アーキテクチャ。

【請求項91】 請求項90記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、更に、前記ライセンスを前記暗号化デジタル・コンテンツに結び付けるデジタル署名を含む、アーキテクチャ。

【請求項92】 請求項83記載のアーキテクチャにおいて、前記DRMシステムが、前記計算機に格納されておりかつ前記デジタル・コンテンツに対応するいずれのデジタル・ライセンスに基づいても、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、計算機のユーザを前記ライセンス・サーバに差し向け、求められた態様でこのようなデジタル・コンテンツをレンダリングするデジタル・ライセンスを取得させる、アーキテクチャ。

【請求項93】 請求項83記載のアーキテクチャにおいて、前記DRMシステムが、前記計算機に格納されておりかつ前記デジタル・コンテンツに対応するいずれのデジタル・ライセンスに基づいても、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、前記DRMシステムは、計算機のユーザ側には何の行為を必要とせずに、前記ライセンス・サーバからデジタル・ライセンスを透過的に取得する、アーキテクチャ。

【請求項94】 請求項83記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスをこのようなデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項95】 請求項94記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスを、公開／秘密鍵技術によって、このようなデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項96】 請求項83記載のアーキテクチャにおいて、前記ライセンス・サーバは、DRMシステムが前記ライセンスを順守することを当該ライセンス・サーバが信用する場合にのみ、このようなDRMシステムにデジタル・ライ

センスを発行する、アーキテクチャ。

【請求項97】 請求項96記載のアーキテクチャにおいて、前記コンテンツ・サーバは、前記デジタル・コンテンツを暗号化形態で配布し、前記DRMシステムは、このようなDRMシステムのために解読および暗号化機能を実行する信頼ブラック・ボックスを含み、前記ブラック・ボックスは、前記解読および暗号化機能を実行するために、一意の公開／秘密鍵対を含み、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求がブラック・ボックス公開鍵を含み、前記ライセンス・サーバは、このようなライセンスの発行に先立って、前記ブラック・ボックス公開鍵にしたがって前記デジタル・ライセンスの少なくとも一部を暗号化することにより、このようなライセンスをこのようなブラック・ボックスに結び付ける、アーキテクチャ。

【請求項98】 請求項97記載のアーキテクチャにおいて、前記コンテンツ・サーバは前記デジタル・コンテンツを暗号化形態で配布し、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、前記暗号化デジタル・コンテンツを解読する解読鍵を含み、前記ライセンス・サーバは、前記ブラック・ボックス公開鍵にしたがって前記ライセンスにおける解読鍵を暗号化する、アーキテクチャ。

【請求項99】 請求項98記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、更に、前記ライセンスによって与えられる権利の記述を含み、前記ライセンス・サーバからこのようなライセンスを取得しなければ、前記暗号化デジタル・コンテンツを解読しレンダリングすることが不可能であり、前記ライセンス・サーバは前記解読鍵にしたがって前記ライセンスにおける権利の記述を暗号化する、アーキテクチャ。

【請求項100】 請求項97記載のアーキテクチャにおいて、前記ブラック・ボックスはバージョン番号を含み、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求が前記ブラック・ボックスのバージョン番号を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記ブラック・ボックス

のバージョン番号が容認可能か否か判定を行い、前記ライセンス・サーバは、前記ブラック・ボックスのバージョン番号が容認可能でないと判定したとき、前記ブラック・ボックスが更新されるまで、前記ライセンスの発行を拒絶し、前記アーキテクチャは、更に、更新ブラック・ボックスを前記DRMシステムに供給するブラック・ボックス・サーバを備える、アーキテクチャ。

【請求項101】 請求項9記載のアーキテクチャにおいて、前記ブラック・ボックスは、承認された証明機関によって供給される証明機関署名を含み、前記ライセンス・サーバは、前記DRMシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求が前記証明機関署名を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記証明機関署名が有効か否か判定を行なう、アーキテクチャ。

【請求項102】 請求項9記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、前記ライセンスによって与えられる権利の記述を含み、前記DRMシステムは、前記権利の記述を評価し、レンダリング・アプリケーションによるデジタル・コンテンツのレンダリングが前記ライセンスの権利の記述に応じたものである場合、このようなレンダリングを許可する、信頼ライセンス評価部を含む、アーキテクチャ。

【請求項103】 請求項8記載のアーキテクチャであって、更に、前記ライセンス・サーバが発行するデジタル・ライセンスに関する情報を維持する発行ライセンス・データベースを備え、前記計算機が受信したライセンスを紛失した場合、前記発行ライセンス・データベースにおける情報に基づいて、その再発行を可能とした、アーキテクチャ。

【請求項104】 請求項8記載のアーキテクチャにおいて、前記オーサリング・ツールは、解読鍵にしたがって前記デジタル・コンテンツを暗号化し、前記デジタル・コンテンツおよび前記暗号化鍵に関する情報をコンテンツ鍵データベースに格納する、アーキテクチャ。

【請求項105】 請求項104記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記デジタル・コンテンツに対応するライセンスの発行に先立って、前記コンテンツ鍵データベース内にある前記デジタル・コンテンツおよ

び前記暗号化鍵に関する情報にアクセスし、このようなライセンスの発行に伴う前記解読鍵を含む、アーキテクチャ。

【発明の詳細な説明】**【0001】**

(関連出願に対する引用)

本願は、“ENFORCEMENT ARCHITECTURE AND METHOD FOR DIGITAL RIGHTS MANAGEMENT”(デジタル権利管理実施アーキテクチャおよび方法)と題し、弁理士整理番号MSFT-0063の下で1999年3月27日に出願した米国仮出願第60/126,614号の優先権を主張する。

【0002】

(発明の分野)

本発明は、デジタル・コンテンツにおける権利実施アーキテクチャに関する。更に特定すれば、本発明は、デジタル・コンテンツのユーザが取得した実施権(licence right)によって指定されるパラメータのみに応じて暗号化デジタル・コンテンツに対するアクセスを許可するようにした、実施アーキテクチャに関する。

【0003】

(発明の背景)

デジタル権利の管理および実施は、デジタル・オーディオ、デジタル・ビデオ、デジタル・テキスト、デジタル・データ、デジタル・マルチメディア等のようなデジタル・コンテンツに関して、このようなデジタル・コンテンツをユーザに配付する場合に非常に望ましい。典型的な配付方式は、磁気(フロッピー)ディスク、磁気テープ、光(コンパクト)ディスク(CD)等のような有形デバイスや、電子掲示板、電子ネットワーク、インターネット等のような無形媒体を含む。ユーザが受信すると、ユーザはメディア・プレーヤ、パーソナル・コンピュータのような適当なレンダリング・デバイスの助けによって、デジタル・コンテンツのレンダリング(rendering)即ち「再生」を行なう。

【0004】

典型的に、コンテンツ所有者即ち著作者、出版社、放送会社等(以下「コンテンツ所有者」)のような権利保有者は、このようなデジタル・コンテンツをライセンス料またはその他の何らかの対価との交換によってユーザ即ち受取人に販売

したい。このようなコンテンツ所有者は、選択が認められれば、ユーザがこのように販売したデジタル・コンテンツを用いて行なえることを制限したいことも多いであろう。例えば、コンテンツ所有者は、ユーザがこのようなコンテンツをコピーしたり、第2のユーザに再配付することを、少なくともこのような第2のユーザがコンテンツ所有者にライセンス料を拒否するような態様では、制約したいであろう。

【0005】

加えて、コンテンツ所有者は、異なるライセンス料で異なる種類の使用許諾を購入する柔軟性をユーザに提供しつつ、同時に実際にいかなるライセンスの種類を購入しようがユーザにその条件を維持させたいこともある。例えば、コンテンツ所有者は、販売したデジタル・コンテンツの再生を限定回数のみ、ある合計時間だけ、ある種の機械においてのみ、ある種のメディア・プレーヤにおいてのみ、ある種のユーザにのみ再生することを許可したい場合もある。

【0006】

しかしながら、販売を行なった後、このようなコンテンツ所有者は、デジタル・コンテンツの管理を行なうにしても、極僅かである。これは、特に、実際にあらゆる新製品または最新のパーソナル・コンピュータが、このようなデジタル・コンテンツの正確なデジタル・コピーを作成するため、ならびにこのような正確なデジタル・コピーを書き込み可能な磁気または光ディスクにダウンロードするため、またはこのような正確なコピーをあらゆる宛先にインターネットのようなネットワークを通じて送るために必要なソフトウェアおよびハードウェアを含んでいるという事実を考慮すると、問題である。

【0007】

勿論、ライセンス料が得られた場合法的処置の一部として、コンテンツ所有者はデジタル・コンテンツのユーザに、このようなデジタル・コンテンツの再配付をしないことを約束するように求めることはできる。しかしながら、このような約束は容易に行われ、容易に破られる。コンテンツ所有者は、大抵の場合暗号化および解読を伴う、いくつかの公知のセキュリティ・デバイスのいずれかによってこのような再配付を防止しようとすることもできる。しかしながら、決意の弱

いユーザ (mildly determined user) に、暗号化デジタル・コンテンツを解読し、このようなデジタル・コンテンツを無暗号化形態で保存し、次いでこれを再配付する、ということを禁止できない場合が多い。

【0008】

したがって、デジタル・コンテンツの任意の形態のレンダリング即ち再生を管理可能にする実施アーキテクチャおよび方法を提供する必要がある。この場合、管理は柔軟性があり、このようなデジタル・コンテンツのコンテンツ所有者によって定義可能とする。また、パーソナル・コンピュータのような計算機上においてレンダリング環境を管理する必要性もある。この場合、レンダリング環境は、このような実施アーキテクチャの少なくとも一部を含む。このようなレンダリング環境の管理によって、デジタル・コンテンツはコンテンツ所有者の制御下にはない計算機上でレンダリングされるものの、コンテンツ所有者が指定するようにのみデジタル・コンテンツをレンダリングすることが可能になる。

【0009】

更に、計算機上において信頼コンポーネント (trusted component) を走らせ、このような計算機のユーザがコンテンツ所有者が許可しない方法でこのようなデジタル・コンテンツにアクセスしようとしても、信頼コンポーネントがコンテンツ所有者の権利を、1 片のデジタル・コンテンツに関してこのような計算機上で実施することも必要とされている。単なる一例として、このような信頼ソフトウェア・コンポーネントは、計算機のユーザが、コンテンツ所有者が許可する場合を除いて、このようなデジタル・コンテンツのコピーを作成することを防止する。

(発明の概要)

前述の必要性は、少なくとも部分的にデジタル権利管理実施アーキテクチャおよび方法によって満たされる。このアーキテクチャおよび方法は、インターネット、光ディスク等において利用可能な保護 (保証) デジタル・コンテンツにおいて権利を実施する。コンテンツを利用可能にするために、アーキテクチャは、コンテンツ・サーバを含み、ここからインターネット等を通じて暗号化した形態でデジタル・コンテンツにアクセス可能である。コンテンツ・サーバは、暗号化デ

ジタル・コンテンツを供給し、光ディスク等に記録することも可能であり、暗号化デジタル・コンテンツは光ディスク自体で配付することもできる。コンテンツ・サーバでは、デジタル・コンテンツを暗号化鍵を用いて暗号化し、公開／秘密鍵技術を用いて、ユーザの計算機またはクライアント・マシン上でデジタル・コンテンツをデジタル・ライセンスと結び付ける。

【0010】

ユーザがデジタル・コンテンツを計算機上でレンダリングしようとする、レンダリング・アプリケーションが、このようなユーザの計算機上でデジタル権利管理(DRM)システムを呼び出す。ユーザが最初にデジタル・コンテンツをレンダリングしようとしている場合、DRMシステムはユーザをライセンス・サーバに差し向け、このようなデジタル・コンテンツをレンダリングするライセンスを、求められた態様で取得させるか、あるいはユーザ側では何の行為も必要とせず、このようなライセンス・サーバからこのようなライセンスを透過的に取得する。ライセンスは以下を含む。

【0011】

ー暗号化デジタル・コンテンツを解読する解読鍵(KD)

ーライセンスおよび関連条件(開始日、終了日、再生回数等)によって与えられる権利(再生、コピー等)の記述。このような記述はデジタル的に読み取り可能な形態である。

【0012】

ーライセンスの保全を確保するデジタル署名

ユーザは、このようなライセンスをライセンス・サーバから取得しなければ、暗号化デジタル・コンテンツの解読やレンダリングを行なうことができない。取得したライセンスは、ユーザの計算機においてライセンス・ストアに格納される。

【0013】

重要なことは、ライセンス・サーバは「信頼」された(即ち、それ自体で認証可能な)DRMシステムにライセンスを発行するだけであるということである。

「信頼」を築くために、DRMシステムには「ブラック・ボックス」が装備され

ており、これがこのようなDRMシステムのために解読および暗号化機能を実行する。ブラック・ボックスは、公開／秘密鍵対、バージョン番号、および一意の署名を含み、これらは全て承認された証明機関によって供給される。公開鍵は、発行されたライセンスの一部を暗号化する目的でライセンス・サーバに使用可能とされ、これによってこのようなライセンスをこのようなブラック・ボックスに結び付ける。秘密鍵は、対応する公開鍵で暗号化した情報を解読する目的のために、ブラック・ボックスにのみ使用可能であり、ユーザやその他の誰にも使用できない。最初に、DRMシステムには公開／秘密鍵対を有するブラック・ボックスが供給され、ユーザが最初にライセンスを要求するときに、更新した保証ブラック・ボックスをブラック・ボックス・サーバからダウンロードするようにユーザに促す。ブラック・ボックス・サーバは、一意の公開／秘密鍵対と共に、更新ブラック・ボックスを供給する。このような更新ブラック・ボックスは、一意の実行可能コードで書かれており、ユーザの計算機上でのみ走り、定期的に再更新される。ユーザがライセンスを要求すると、クライアント・マシンはブラック・ボックス公開鍵、バージョン番号、および署名をライセンス・サーバに送り、そしてこのようなライセンス・サーバは、バージョン番号が現行であり署名が有効な場合、ライセンスを発行する。また、ライセンス要求は、ライセンスを要求するデジタル・コンテンツの識別、および要求したデジタル・コンテンツに関連する解読鍵を識別する鍵IDも含む。ライセンス・サーバは、ブラック・ボックス公開鍵を用いて解読鍵を暗号化し、解読鍵を用いてライセンス条件を暗号化し、次いで暗号化した解読鍵および暗号化したライセンス条件を、ライセンス署名と共に、ユーザの計算機にダウンロードする。

【0014】

一旦ダウンロードしたライセンスをDRMシステムのライセンス・ストアに格納したなら、ユーザはライセンスによって与えられライセンス条件において指定された権利にしたがって、デジタル・コンテンツをレンダリングすることができる。デジタル・コンテンツをレンダリングする要求が行われると、ブラック・ボックスに解読鍵およびライセンス条件を解読させ、DRMシステムのライセンス評価部がこのようなライセンス条件を評価する。ブラック・ボックスは、ライセ

ンスの評価の結果、要求元にこのようなコンテンツを再生することを許可すると判断した場合にのみ、暗号化デジタル・コンテンツを解読する。解読したコンテンツは、レンダリング・アプリケーションに供給され、レンダリングが行われる。

(図面の簡単な説明)

前述の概要、および以下の本発明の実施形態の更に詳細な説明は、添付図面と関連付けて読むことにより、一層理解が深まるであろう。本発明を例示する目的のために、現在好適な実施形態を図面に示す。しかしながら、当然理解されるであろうが、本発明は図示する構成や手段そのものに限定される訳ではない。

(発明の詳細な説明)

図面を詳細に参照すると、全体を通じて同様のエレメントを示すために同様の番号が用いられている。図1には、本発明の一実施形態による実施アーキテクチャ10を示す。概略的に、実施アーキテクチャ10は、デジタル・コンテンツ12の所有者にライセンス規則を指定させ、このライセンス規則を満たさなければ、ユーザの計算機14上でこのようなデジタル・コンテンツ12をレンダリングすることが許可されない。このようなライセンス規則は、デジタル・ライセンス16に具体化され、ユーザ/ユーザの計算機14（以後、このような用語は、特に状況が必要としない限り、相互交換可能とする）は、コンテンツ所有者またはその代理人から取得しなければならない。デジタル・コンテンツ12は、暗号化した形態で配付され、自由に広く配付することもできる。好ましくは、デジタル・コンテンツ12を解読するための解読鍵(KD)をライセンス16と共に含ませる。

計算機環境

図12および以下の論述は、本発明を実現するのに適した計算機環境の端的な一般的な説明を行なうことを意図している。必ずしもその必要はないが、本発明の説明は、少なくとも部分的には、プログラム・モジュールのような、クライアント・ワークステーションまたはサーバのようなコンピュータが実行する一般的なコンピュータ実行可能命令に関連して行なう。一般に、プログラム・モジュールは、ルーチン・プログラム、オブジェクト、コンポーネント、データ構造等を

含み、特定のタスクを実行したり、あるいは特定の抽象的データ・タイプを実装する。更に、本発明およびその一部は、ハンド・ヘルド・デバイス、マルチプロセッサ・システム、マイクロプロセッサ系電子機器またはプログラマブル消費者電子機器、ネットワークPC、ミニコンピュータ、メインフレーム・コンピュータ等を含む、別のコンピュータ・システム構成でも実施可能であることも認めよう。また、本発明は、分散型計算機環境においても実施可能であり、この場合、通信ネットワークを通じてリンクされたりリモート処理デバイスによってタスクを実行する。分散型計算機環境では、プログラム・モジュールは、ローカルおよびリモート・メモリ記憶装置双方に位置することができる。

【0015】

図12に示すように、本発明を実現する汎用計算機システムの一例は、従来のパーソナル・コンピュータ120等を含む。このパーソナル・コンピュータ120は、演算装置121、システム・メモリ122、およびシステム・メモリから演算装置121までを含む種々のシステム・コンポーネントを結合するシステム・バス123を含む。システム・バス123は、数種類のバス構造のいずれでもよく、メモリ・バスまたはメモリ・コントローラ、周辺バス、および種々のバス構造のいずれかをを用いてローカル・バスが含まれる。システム・メモリは、リード・オンリ・メモリ（ROM）124およびランダム・アクセス・メモリ（RAM）125を含む。基本入出力システム126（BIOS）は、起動中のように、パーソナル・コンピュータ120内のエレメント間におけるデータ転送を補助する基本的なルーティンを含み、ROM124内に格納されている。

【0016】

更に、パーソナル・コンピュータ120は、図示しないハード・ディスクの読み書きを行なうハード・ディスク・ドライブ127、リムーバブル磁気ディスク129の読み書きを行なう磁気ディスク・ドライブ128、CD-ROMまたはその他の光媒体のようなリムーバブル光ディスク131の読み書きを行なう光ディスク・ドライブ130のような種々の周辺ハードウェア・デバイスも含む。ハード・ディスク・ドライブ127、磁気ディスク・ドライブ128、および光ディスク・ドライブ130は、それぞれ、ハード・ディスク・ドライブ・インター

フェース132、磁気ディスク・ドライブ・インターフェース133、および光ドライブ・インターフェース134を介して、システム・バス123に接続されている。ドライブおよびそれに関連するコンピュータ読取可能媒体は、コンピュータ読取可能命令、データ構造、プログラム・モジュールおよびパーソナル・コンピュータ20のその他のデータの不揮発性格納を行なう。

【0017】

ここに記載する環境の一例は、ハード・ディスク、リムーバブル磁気ディスク129およびリムーバブル光ディスク131を採用するが、コンピュータによるアクセスが可能なデータを格納することができる、別の形式のコンピュータ読取可能媒体も、動作環境例では使用可能であることは、当業者には認められよう。このような他の形式の媒体は、磁気カセット、フラッシュ・メモリ・カード、デジタル・ビデオ・ディスク、ベルヌーイ・カートリッジ、ランダム・アクセス・メモリ(RAM)、リード・オンリ・メモリ(ROM)等を含む。

【0018】

ハード・ディスク、磁気ディスク129、光ディスク131、ROM124またはRAM125上には、多数のプログラム・モジュールを格納可能であり、オペレーティング・システム135、1つ以上のアプリケーション・プログラム136、その他のプログラム・モジュール137、およびプログラム・データ138を含む。ユーザは、キーボード140およびポインティング・デバイス142のような入力デバイスによって、コマンドおよび情報をパーソナル・コンピュータ20に入力することができる。他の入力デバイス(図示せず)は、マイクロフォン、ジョイスティック、ゲーム・パッド、衛星ディッシュ、スキャナ等を含むことができる。これらおよびその他の入力デバイスは、多くの場合、システム・バスに結合するシリアル・ポート・インターフェース146を介して、演算装置121に接続されるが、パラレル・ポート、ゲーム・ポートまたはユニバーサル・シリアル・バス(USB)のようなその他のインターフェースによって接続することも可能である。また、ビデオ・アダプタ148のような周辺ハードウェア・インターフェース・デバイスを介して、モニタ147またはその他の種類のディスプレイ装置もシステム・バス123に接続してある。モニタ147に加えて

、パーソナル・コンピュータは、典型的に、スピーカおよびプリンタのような、その他の周辺出力デバイス（図示せず）を含む。図12のシステム例は、ホスト・アダプタ155、小型コンピュータ・システム・インターフェース（SCSI）バス156、およびSCSIバス156に接続されている外部記憶装置162も含む。

【0019】

パーソナル・コンピュータ120は、リモート・コンピュータ149のような1つ以上のリモート・コンピュータへの論理接続を用いれば、ネットワーク環境においても動作可能である。リモート・コンピュータ149は、別のパーソナル・コンピュータ、サーバ、ルータ、ネットワークPC、ピア・デバイス、またはその他の共通ネットワーク・ノードとすることができ、典型的に、パーソナル・コンピュータ120に関して先に述べたエレメントの多くまたは全てを含むが、図12にはメモリ記憶装置150のみを図示している。図12に示す論理接続は、ローカル・エリア・ネットワーク（LAN）151およびワイド・エリア・ネットワーク（WAN）152を含む。このようなネットワーク環境は、会社全域に及ぶコンピュータ・ネットワーク、イントラネットおよびインターネットでは一般的である。

【0020】

LANネットワーク環境で用いる場合、パーソナル・コンピュータ120は、ネットワーク・インターフェースまたはアダプタ153を介してローカル・ネットワーク151に接続する。WANネットワーク環境で用いる場合、パーソナル・コンピュータ120は、典型的に、モデム154、またはインターネットのようなワイド・エリア・ネットワーク52を通じて通信を確立する、その他の手段を含む。モデム154は、内蔵型でも外付けでもよく、シリアル・ポート・インターフェース146を介してシステム・バス123に接続する。ネットワーク環境では、パーソナル・コンピュータ120に関して図示したプログラム・モジュールまたはその一部は、ローカルまたはリモートメモリ記憶装置に格納することもできる。尚、図示のネットワーク接続は一例であり、コンピュータ間に通信リンクを確立する別の手段も使用可能であることは認められよう。

アーキテクチャ

再度図1を参照すると、本発明の一実施形態において、アーキテクチャ10は、前述のユーザの計算機14だけでなく、オーサリング・ツール18、コンテンツ鍵データベース20、コンテンツ・サーバ22、ライセンス・サーバ24、およびブラック・ボックス・サーバ25を含む。

アーキテクチャーオーサリング・ツール18

オーサリング・ツール18は、コンテンツ所有者が1片のデジタル・コンテンツ12を、本発明のアーキテクチャ10と共に使用可能な形態にパッケージ化するために用いられる。即ち、コンテンツ所有者は、オーサリング・ツール18に、デジタル・コンテンツ12、ならびに当該デジタル・コンテンツ12に付随する命令および／または規則、ならびにデジタル・コンテンツ12をどのようにパッケージ化するかに関する命令および／または規則を供給する。すると、オーサリング・ツール18は、暗号化／解読鍵にしたがって暗号化したデジタル・コンテンツ12、およびデジタル・コンテンツ12に付随する命令および／または規則を有するデジタル・コンテンツ・パッケージ12pを生成する。

【0021】

本発明の一実施形態では、オーサリング・ツール18は、いくつかの異なるデジタル・コンテンツ12のパッケージ12pを連続して生成するように命令され、その各々が、異なる暗号化／解読鍵にしたがって暗号化された同じデジタル・コンテンツを有する。当然理解されようが、デジタル・コンテンツ12が同じである数個の異なるパッケージ12pを有することは、このようなパッケージ12p／コンテンツ12（以後、特に状況が必要としない限り、単に「デジタル・コンテンツ12」）の配付を追跡する際に有用となり得る。このような配付追跡は、通常は必要でないが、デジタル・コンテンツ12が不法に販売または放送された場合には、調査機関が用いることができる。

【0022】

本発明の一実施形態では、デジタル・コンテンツ12を暗号化する暗号化／解読鍵は、対称鍵であり、暗号化鍵が解読鍵（KD）にもなる。以下で更に詳しく論ずるが、このような解読鍵（KD）は、このようなデジタル・コンテンツ12

のライセンス16の一部として、隠された形態でユーザの計算機14に配信される。好ましくは、各デジタル・コンテンツ12片には、コンテンツIDが備えられており（または、各パッケージ12pにはパッケージIDが備えられており）、各解読鍵（KD）は鍵IDを有し、オーサリング・ツール18によって、各デジタル・コンテンツ12片毎に（または各パッケージ12p毎に）解読鍵（KD）、鍵ID、およびコンテンツID（またはパッケージID）を鍵コンテンツ・データベース20に格納する。加えて、デジタル・コンテンツ12に対して発行されるライセンス16の種類、ならびにライセンス16の各種類に対する条件（terms and conditions）に関するライセンス・データも、コンテンツ鍵データベース20、またはその他のデータベース（図示せず）に格納することができる。好ましくは、ライセンス・データは、後に、状況およびマーケット条件の要求に応じて、コンテンツ所有者によって変更することができる。

【0023】

使用においては、オーサリング・ツール18には、とりわけ、次の項目を含む情報が供給される。

ーパッケージ化するデジタル・コンテンツ12

ー必要であれば、用いる透かしおよび／または指紋の形式およびパラメータ、

ー必要であれば、用いるデータ圧縮の形式およびパラメータ、

ー用いる暗号化の形式およびパラメータ、

ー必要であれば、用いるシリアル化の形式およびパラメータ、および

ーデジタル・コンテンツ12に伴う命令および／または規則。

【0024】

公知のように、透かしとは、隠されたコンピュータ読み取り可能信号であり、識別子としてデジタル・コンテンツ12に追加される。指紋とは、各インスタンス毎に異なる透かしのことである。当然理解されようが、インスタンスとは、一意であるデジタル・コンテンツ12のバージョンである。いずれのインスタンスでも、そのコピーを多数作成することができ、いずれのコピーも特定のインスタンスを有する。デジタル・コンテンツ12の特定のインスタンスが不法に販売または放送された場合、調査機関は、このようなデジタル・コンテンツ12に付加

されている透かし／指紋にしたがって十中八九容疑者を特定することができる。

【0025】

データ圧縮は、本発明の精神および範囲から逸脱することなく、適切な圧縮アルゴリズムであればそのいずれにしたがって実施することも可能である。例えば、.mp3または、wav圧縮アルゴリズムを用いることができる。勿論、デジタル・コンテンツ12は、既に圧縮状態であってもよく、この場合追加の圧縮は不要である。

【0026】

デジタル・コンテンツ12に伴うべき命令／および規則は、實際上、本発明の精神および範囲から逸脱することなく、適切であればあらゆる命令、規則、またはその他の情報を含むことができる。以下で論ずるが、このような付随する命令／規則／情報は、主にユーザおよびユーザの計算機14によって、ライセンス16を取得し、デジタル・コンテンツ12をレンダリングするために用いられる。したがって、このような付随命令／規則／情報は、適切にフォーマットされたライセンス取得スクリプト等を含むことができる。これについては、以下で更に詳しく説明する。加えて、または代わりに、このような付随命令／規則／情報は、デジタル・コンテンツ12のプレビューをユーザに与えるように設計した、「プレビュー」情報を含むこともできる。

【0027】

次に、供給された情報を用いて、オーサリング・ツール18は、デジタル・コンテンツ12に対応する1つ以上のパッケージ12pを生成する。各パッケージ12pは、次に、コンテンツ・サーバ2に格納され、世界中に配付される。

【0028】

本発明の一実施形態において、図2をここで参照すると、オーサリング・ツール18は、ダイナミック・オーサリング・ツール18であり、入力パラメータを受け取る。これらは、オーサリング・ツール18上で指定し、動作させることができる。したがって、このようなオーサリング・ツール18は、多数片のデジタル・コンテンツ12に対して、パッケージ12pの多数の変形を迅速に生成することができる。好ましくは、入力パラメータは、図示のように、辞書28の形態

で具体化する。ここで、辞書28は、以下のようなパラメータを含む。

【0029】

ーデジタル・コンテンツ12を有する入力ファイル29aの名称、
ー行われるエンコードの形式、
ー用いる暗号化／解読鍵(KD)、
ーパッケージ12p内にデジタル・コンテンツ12と共にパッケージ化する付随命令／規則／情報(「ヘッダ情報」)、
ー行なわれる多重化(muxing)の形式、および
ーデジタル・コンテンツ12に基づくパッケージ12pを書き込む出力ファイル29bの名称。

【0030】

当然理解されようが、このような辞書28は、オーサリング・ツール18のオペレータ(人間または機械)によって容易にかつ素早く変更可能であり、したがって、オーサリング・ツール18によって実行するオーサリングの形式も、容易にかつ素早く、動的に変更可能である。本発明の一実施形態では、オーサリング・ツール18は、コンピュータ画面上において人のオペレータに閲覧可能なオペレータ・インターフェース(図示せず)を含む。したがって、このようなオペレータは、インターフェースを通じて辞書28を変更することができ、更にインターフェースによる辞書28の変更を適切に補助したり、あるいは規制することも可能である。

【0031】

オーサリング・ツール18では、図2に見られるように、ソース・ファイル18aは、辞書28からデジタル・コンテンツ12を有する入力ファイル29aの名称を検索し、RAMのようなメモリ29cにデジタル・コンテンツ12を置く。エンコード・フィルタ18bは、次に、メモリ29c内のデジタル・コンテンツ12に対してエンコードを行い、入力フォーマットから、辞書28において指定されているエンコード形式に応じた出力フォーマット(即ち、.wavから、.asp、.mp3から、.asp、等)にファイルを転送し、エンコードしたデジタル・コンテンツ12をメモリ29c内に置く。図示のように、パッケージ化する

るデジタル・コンテンツ12（例えば、音楽）は、. wavまたは、mp3フォーマットのような圧縮フォーマットで受け取られ、. asp（アクティブ・ストリーミング・プロトコル）フォーマットのようなフォーマットに変換される。勿論、その他の入力および出力フォーマットも採用でき、本発明の精神および範囲から逸脱する訳ではない。

【0032】

その後、暗号化フィルタ18cがメモリ29c内のエンコード・デジタル・コンテンツ12を、辞書28において指定されている暗号化／解読鍵（KD）にしたがって暗号化し、暗号化したデジタル・コンテンツ12をメモリ29c内に置く。次に、ヘッダ・フィルタ18dが、辞書28において指定されているヘッダ情報を、メモリ29c内の暗号化デジタル・コンテンツ12に追加する。

【0033】

当然理解されようが、状況に応じて、パッケージ12pは、時間的に整合したデジタル・コンテンツ12の多数のストリームを含む場合もある（1つのストリームを図2に示す）。このような多数のストリームは多重化されている（即ち「muxed」）。したがって、多重化フィルタ18eは、辞書28において指定されている多重化形式にしたがって、メモリ29c内のヘッダ情報および暗号化デジタル・コンテンツ12の多重化を行い、その結果をメモリ29cに置く。次に、ファイル書き込みフィルタ18fが、メモリ29cからこの結果を検索し、このような結果を、パッケージ12pとして辞書28に指定されている出力ファイル29bに書き込む。

【0034】

尚、ある状況においては、実行するエンコードの形式は通常では変更しないことを注記しておく。多重化形式は典型的にエンコード形式に基づくので、多重化形式も通常では同様に変更しない。実際にそういう場合には、辞書28は、エンコード形式および多重化形式に関するパラメータを含む必要はない。代わりに、エンコード形式をエンコード・フィルタに「ハードワイヤ」し、あるいは多重化形式を多重化フィルタに「ハードワイヤ」するだけでよい。勿論、状況が要求する場合には、オーサリング・ツール18は前述のフィルタ全てを含まなくてもよ

く、あるいは他のフィルタを含んでもよく、含んだフィルタは、ハードワイヤにしても、辞書28内で指定されているパラメータにしたがってその機能を実行してもよく、全て本発明の精神および範囲から逸脱することはない。

【0035】

好ましくは、オーサリング・ツール18は、適切なソフトウェアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような計算機およびこのようなソフトウェアの構造および動作は、この開示に基づけば明白なはずであり、したがって本開示において更に詳しい論述は必要でない。

アーキテクチャー・コンテンツ・サーバ22

再度図1を参照すると、本発明の一実施形態において、コンテンツ・サーバ22は、オーサリングツール18が生成したパッケージを配布するか、またはその他の方法で検索できるようにする。このようなパッケージ12pは、適切な配布チャネルのいずれかを通じて、コンテンツ・サーバ22の要求に応じて配布することができ、本発明の精神および範囲から逸脱することはない。例えば、このような配布チャネルは、インターネットまたはその他のネットワーク、電子掲示板、電子メール等とすることもできる。加えて、コンテンツ・サーバ22を用いて、パッケージ12pを磁気または光ディスクあるいはその他の記憶装置にコピーすることもでき、このような記憶装置を配付してもよい。

【0036】

尚、コンテンツ・サーバ22は、いずれの信頼またはセキュリティ問題にも関係なく、パッケージを配布することは認められよう。以下で論ずるが、このような問題は、ライセンス・サーバ24およびこのようなライセンス・サーバ24とユーザのコンピュータ14との間の関係と関連付けて扱われる。本発明の一実施形態では、コンテンツ・サーバ22は自由に、デジタル・コンテンツ12を有するパッケージ12pを、これを要求するあらゆる配布先にリリースし、配布する。しかしながら、コンテンツ・サーバ22は、このようなパッケージ12pのリリースおよび配布に制約を設けることもでき、本発明の精神および範囲から逸脱する訳ではない。例えば、コンテンツ・サーバ22は、配布前に、所定の配布料の支払を

最初に要求することもでき、あるいは配布先にそれ自体を同定することを要求することもでき、あるいは配布先の識別に基づいて配布を行なうか否か実際に判断することもできる。

【0037】

加えて、コンテンツ・サーバ22を用いて、オーサリング・ツール18を制御することによって在庫管理を行い、予めある数の異なるパッケージ12pを生成し、予測される需要を満たすようにすることもできる。例えば、サーバは、同じデジタル・コンテンツ12に基づいて100個のパッケージ12pを生成し、各パッケージ12pを10回送達することもできる。パッケージ12pの供給が例えば、20に減少すると、コンテンツ・サーバ22はオーサリング・ツール18に、例えば、80個の追加パッケージ12pを再度生成するように指令することもできる。

【0038】

好ましくは、アーキテクチャ10内のコンテンツ・サーバ22は、一意の公開／秘密鍵対(PU-C S, PR-C S)を有し、これをライセンス16を評価し、対応するデジタル・コンテンツ12を解読するための解読鍵(KD)を取得するプロセスの一部として採用する。これについては、以下で更に詳しく説明する。公知のように、公開／秘密鍵対は非対称鍵であり、鍵対における鍵の一方で暗号化されるものは、鍵対における鍵の他方を用いなければ解読することができない。公開／秘密鍵対暗号化システムでは、公開鍵は世界中に知らせることができるが、秘密鍵は、このような秘密鍵の所有者によって常に秘密に保持されていなければならない。したがって、コンテンツ・サーバ22がその秘密鍵(PR-C S)でデータを暗号化する場合、解読の目的のためにその公開鍵(PU-C S)と共に、暗号化したデータを世界に送ることができる。対応して、外部デバイスがデータをコンテンツ・サーバ22に送り、このようなコンテンツ・サーバ22のみがこのようなデータを解読するようにしたい場合、このような外部デバイスは最初にコンテンツ・サーバ22の公開鍵(PU-C S)を取得し、次いでこのような公開鍵でデータを暗号化しなければならない。したがって、コンテンツ・サーバ22(そして、コンテンツ・サーバ22のみ)がその秘密鍵(PR-C S

）を用いて、このような暗号化データを解読することができる。

【0039】

オーサリング・ツール18の場合と同様、コンテンツ・サーバ22は、適切なソフトウェアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウェアの構造および動作は、ここの開示に基づいて明らかなはずであるので、本開示では詳細な説明は全く必要ない。更に、本発明の一実施形態では、オーサリング・ツール18およびコンテンツ・サーバ22は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。更に、コンテンツ・サーバ22は、ある状況によっては、オーサリング・ツール18を含み、先に論じたように、オーサリング・ツール18の機能を実行する場合もあることは認められよう。

デジタル・コンテンツ・パッケージ12pの構造

次に図3を参照すると、本発明の一実施形態において、コンテンツ・サーバ22によって配布されるデジタル・コンテンツ・パッケージ12pは次を含む。

【0040】

一先に論じたように暗号化／解読鍵(KD)を用いて暗号化されたデジタル・コンテンツ(即ち、(KD(CONTENT)))、

一このようなデジタル・コンテンツ12(またはパッケージ12p)のコンテンツID(またはパッケージID)、

一解読鍵(KD)の鍵ID、

一好ましくは無暗号化形態のライセンス取得情報、および

一コンテンツ・サーバ22の秘密鍵(PRCS)によって署名された、コンテンツ・サーバ22の公開鍵(PUCS)を暗号化する鍵KD(即ち、(KD(PUCS)S(PRCS)))。

【0041】

(KD(PUCS)S(PRCS))に関して、このような項目は、デジタル・コンテンツ12および／またはパッケージ12pの妥当性検査に関係して用いられることは理解されよう。これについては以下で説明する。デジタル署名

を有する認証（以下を参照のこと）とは異なり、鍵（PU-C S）は（KD（PU-C S））を取得するには必要ではない。代わりに、鍵（PU-C S）は、単に解読鍵（KD）を適用するだけで取得される。一旦こうして取得すれば、このような鍵（PU-C S）は、署名（S（PR-C S））の有効性を検査するために用いることができる。

【0042】

また、このようにオーサリング・ツール18によって構築されるパッケージ12pに対して、このようなオーサリング・ツール18は、恐らくは辞書28から供給されるヘッダ情報として、既にライセンス取得情報および（KD（PU-C S））S（PR-C S））を所持していなければならない。更に、オーサリング・ツール18およびコンテンツ・サーバ22は、恐らくは（KD（PU-C S））S（PR-C S））を構築するために相互作用を行わなければならない。このような相互作用は、例えば、次のステップを含む。

【0043】

ーコンテンツ・サーバ22が（PU-C S）をオーサリング・ツール18に送る。

ーオーサリング・ツール18が（KD）を用いて（PU-C S）を暗号化し、（KD（PU-C S））を生成する。

【0044】

ーオーサリング・ツール18が（KD（PU-C S））をコンテンツ・サーバ22に送る。

ーコンテンツ・サーバ22が（PR-C S）を用いて（KD（PU-C S））に署名し、（KD（PU-C S））S（PR-C S））を生成する。

【0045】

ーコンテンツ・サーバ22が（KD（PU-C S））S（PR-C S））をオーサリング・ツール18に送る。

アーキテクチャーライセンス・サーバ24

再度図1を参照すると、本発明の一実施形態において、ライセンス・サーバ24は、1片のデジタル・コンテンツ12に関して、ユーザの計算機14からライ

センス16の要求を受信し、ユーザの計算機14が、発行するライセンス16を授かることについて信用できるか否か判定を行い、このようなライセンス16を交渉し、このようなライセンス16を作成し、このようなライセンス16をユーザの計算機14に送る機能を実行する。好ましくは、このように送信されるライセンス16は、デジタル・コンテンツ12を解読するための解読鍵(KD)を含む。このようなライセンス・サーバ24およびこのような機能については、以下で更に詳しく説明する。好ましくは、そしてコンテンツ・サーバ22と同様に、アーキテクチャ10におけるライセンス・サーバ24は、一意の公開／秘密鍵対(PU-L S, PR-L S)を有し、ライセンス16を評価するプロセスの一部としてこれを用い、対応するデジタル・コンテンツ12を解読するための解読鍵(KD)を取得する。これについては、以下で更に詳しく説明する。

【0046】

オーサリング・ツール18およびコンテンツ・サーバ22と同様、ライセンス・サーバ24は、適切なソフトウェアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウェアの構造および動作は、ここの開示に基づいて明らかなはずであり、本開示においては詳細な論述は全く不要である。更に、本発明の一実施形態では、オーサリング・ツール18および／またはコンテンツ・サーバ22は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。

【0047】

本発明の一実施形態では、ライセンス16の発行に先立って、ライセンス・サーバ24およびコンテンツ・サーバ22は、代理契約等を行い、ライセンス・サーバ24が実際に、コンテンツ・サーバ22が配布するデジタル・コンテンツ12の少なくとも一部について、ライセンス付与機関(licensing authority)であることに同意する。当然理解されようが、1つのコンテンツ・サーバ22は、数個のライセンス・サーバ24と代理契約を結ぶことができ、あるいは1つのライセンス・サーバ24が数個のコンテンツ・サーバ22と代理契約を結ぶこともでき、いずれも本発明の精神および範囲から逸脱する訳ではない。

【0048】

好ましくは、ライセンス・サーバ24は、実際にそれがコンテンツ・サーバ22によって配布するデジタル・コンテンツ12のライセンス16を発行する代理権を有することを世界に示すことができる。こうすることによって、ライセンス・サーバ24は、コンテンツ・サーバ22に、ライセンス・サーバ24の公開鍵(PULS)を送り、そしてコンテンツ・サーバ22はライセンス・サーバ24に、コンテンツ・サーバ22の秘密鍵(CERT(PULS)S(PRCS))によって署名したコンテンツとして、PULSを含むデジタル認証を送ることが好ましい。当然理解されようが、このような認証におけるコンテンツ(PULS)は、コンテンツ・サーバ22の公開鍵(PRCS)を用いなければ、アクセスすることはできない。当然理解されようが、一般には、基礎となるデータのデジタル署名は、このようなデータの暗号化形態であり、このようなデータが偽造されていたり、あるいはその他の方法で変更されている場合、解読の際にこのようなデータと一致しない。

【0049】

1片のデジタル・コンテンツ12に関連するライセンス代理権として、そしてライセンス付与機能の一部として、ライセンス・サーバ24は、このようなデジタル・コンテンツ12のための解読鍵(KD)にアクセスできなければならない。したがって、ライセンス・サーバ24は、このようなデジタル・コンテンツ12(またはパッケージ12p)に対する解読鍵(KD)、鍵ID、およびコンテンツID(またはパッケージID)を有するコンテンツ鍵データベース20にアクセスすることが好ましい。

アーキテクチャブラック・ボックス・サーバ26

更に図1を参照すると、本発明の一実施形態では、ブラック・ボックス・サーバ26は、ユーザの計算機14において、新たなブラック・ボックス30をインストールし、アップデートする機能を実行する。以下で更に詳しく説明するが、ブラック・ボックス30は、ユーザの計算機14のために、暗号化および解読機能を実行する。また、以下で更に詳しく説明するが、ブラック・ボックス30は、安全であり攻撃から保護されることを想定している。このようなセキュリティ

および保護は、少なくとも部分的に、ブラック・ボックス30を、必要に応じてブラック・ボックス・サーバ26によって新たなバージョンにアップグレードすることによって得られる。これについては、以下で更に詳しく説明する。

【0050】

オーサリング・ツール18、コンテンツ・サーバ22、およびライセンス・サーバ24の場合と同様、ブラック・ボックス・サーバ26は、適切なソフトウェアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウェアの構造および動作は、この開示に基づいて明らかなはずであり、したがって本開示では詳細な論述は不要である。更に、本発明の一実施形態では、ライセンス・サーバ24、オーサリング・ツール18、および/またはコンテンツ・サーバ22は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。しかし、セキュリティの目的上、ブラック・ボックス・サーバ26を別個の機械に有する方が賢明であることを注記しておく。

アーキテクチャーユーザの計算機14

次に図4を参照すると、本発明の一実施形態では、ユーザの計算機14は、パーソナル・コンピュータ等であり、キーボード、マウス、画面、プロセッサ、RAM、ROM、ハード・ドライブ、フロッピー・ドライブ、CDプレーヤ等のようなエレメントを有する。しかしながら、ユーザの計算機14は、とりわけ、テレビジョンまたはモニタのような専用閲覧デバイス、ステレオまたはその他の音楽プレーヤのような専用オーディオ・デバイス、専用プリンタ等でもよく、本発明の精神および範囲から逸脱することはない。

【0051】

1片のデジタル・コンテンツ12のコンテンツ所有者は、ユーザの計算機14が、このようなコンテンツ所有者が指定した規則を固守すること、即ち、求められた態様でレンダリングを許可するライセンス16をユーザが取得しなければ、デジタル・コンテンツ12をレンダリングしないことを信用しなければならない。好ましくは、ユーザの計算機14は、このような計算機14が、デジタル・コンテンツ12に関連しユーザによって取得されたライセンス16に具体化されて

いるライセンス規則にしたがってでなければ、デジタル・コンテンツ12をレンダリングしないことを、コンテンツ所有者に対して履行することができる、信頼(trusted) コンポーネントまたは機構32を備えなければならない。

【0052】

ここで、信頼機構32は、デジタル権利管理(DRM)システム32であり、ユーザが1片のデジタル・コンテンツ12をレンダリングすることを要求したときにイネーブルされ、ユーザが、求められた態様でデジタル・コンテンツ12をレンダリングするライセンス16を有するか否か判定を行い、必要であれば、このようなライセンス16の取得を実施し、ライセンス16にしたがってユーザがデジタル・コンテンツ12を再生する権利を有するか否か判定を行い、実際にユーザがこのようなライセンス16に応じてこのような権利を有する場合、レンダリングの目的で、デジタル・コンテンツ12を解読する。ユーザの計算機14上でのDRMシステム32の内容および機能、およびアーキテクチャ10との関係について、以下に説明する。

DRMシステム32

DRMシステム32は、ここに開示するアーキテクチャ10と共に4つの主要な機能を実行する。(1)コンテンツの取得、(2)ライセンスの取得、(3)コンテンツのレンダリング、および(4)ブラック・ボックス30のインストール/更新である。好ましくは、これらの機能のいずれもいつの時点でも実行することができるが、これらの機能の一部は、デジタル・コンテンツ12が既に取得されていることを要件とすることは認められよう。

DRMシステム32—コンテンツ取得

ユーザおよび/またはユーザの計算機14によるデジタル・コンテンツ12の取得は、典型的に、比較的単純であり、概略的には、暗号化デジタル・コンテンツ12を有するファイルを、ユーザの計算機14上に置くことから成る。勿論、ここに開示するアーキテクチャ10およびDRMシステム32と共に動作するためには、暗号化デジタル・コンテンツ12が、デジタル・パッケージ12pのように、このようなアーキテクチャ10およびDRMシステム32に適した形態であることが必要である。これについては以下で説明する。

【0053】

当然理解されようが、デジタル・コンテンツ12は、コンテンツ・サーバ22から直接的にまたは間接的に、いずれの方法でも取得可能であり、本発明の精神および範囲から逸脱することはない。例えば、このようなデジタル・コンテンツ12は、インターネットのようなネットワークからダウンロードしたり、取得した光または磁気ディスク等に配したり、電子メール・メッセージ等の一部として受信したり、あるいは電子掲示板等からダウンロードすることができる。

【0054】

このようなデジタル・コンテンツ12は、一旦取得すると、計算機14上で走るレンダリング・アプリケーション34（以下で説明する）、およびDRMシステム32によって、取得したデジタル・コンテンツ12がアクセス可能となるように、格納することが好ましい。例えば、デジタル・コンテンツ12は、ユーザの計算機14のハード・ドライブ（図示せず）上、または計算機14にアクセス可能なネットワーク・サーバ（図示せず）上のファイルとして置くこともできる。デジタル・コンテンツ12を光または磁気ディスク等に取得する場合、このようなディスクを、ユーザの計算機14に結合されている適切なドライブ（図示せず）に装填するだけでよい。

【0055】

本発明では、直接配布源としてのコンテンツ・サーバ22からでも、また間接配布源としてのなんらかの仲介物からでも、デジタル・コンテンツ12を取得するために特殊なツールを全く必要としないことを想定している。即ち、デジタル・コンテンツ12は、他のあらゆるデータ・ファイルと同様に容易に取得することが好ましい。しかしながら、DRMシステム32および／またはレンダリング・アプリケーション34は、ユーザがデジタル・コンテンツ12を取得するのを助けるように設計したインターフェース（図示せず）を含むこともできる。例えば、インターフェースは、デジタル・コンテンツ12を探索するように特別に設計したウェブ・ブラウザを含むことができ、デジタル・コンテンツ12のソースであることがわかっている既定のインターネット・ウェブ・サイト等にリンクする。

DRMシステム32-コンテンツ・レンダリング、第1部

図5Aを参照すると、本発明の一実施形態では、暗号化デジタル・コンテンツ12が配布され、ユーザによって受信され、ユーザによって格納ファイルの形態で計算機14上に置かれておりと仮定し、ユーザは、レンダリング・コマンド上である変形 (variation) を実行することによって、デジタル・コンテンツ12をレンダリングしようとする(ステップ501)。例えば、このようなレンダリング・コマンドは、デジタル・コンテンツ12を「再生」または「開く」要求として具体化することができる。計算機環境によっては、例えば、ワシントン州RedmondのMICROSOFT Corporationが販売する“MICROSOFT WINDOWS (登録商標)”オペレーティング・システムのように、このような再生またはオープン・コマンドは、デジタル・コンテンツ12を表わすアイコン上で「クリック」することと同じ位簡単にすることができる。勿論、このようなレンダリング・コマンドのその他の実施形態も採用可能であり、本発明の精神および範囲から逸脱する訳ではない。一般に、このようなレンダリング・コマンドは、ユーザがデジタル・コンテンツ12を有するファイルを開くか、走らせるか、実行する等を指令するときにはいつでも実行するように考慮することができる。

【0056】

重要なことは、そして付加的に、このようなレンダリング・コマンドは、デジタル・コンテンツ12を、印刷形態、視覚形態、聴覚形態等のような別の形態にコピーする要求として具体化できることにある。当然理解されようが、同じデジタル・コンテンツ12を、コンピュータ画面上におけるように、1つの形態でレンダリングし、次いで印刷文書のように別の形態でレンダリングすることもできる。本発明では、各レンダリング形式は、ユーザがそうする権利を有する場合にのみ実行される。これについては以下で説明する。

【0057】

本発明の一実施形態では、デジタル・コンテンツ12は、拡張子で終わるファイル名を有するデジタル・ファイルの形態であり、計算機14は、このような拡張子に基づいて、特定の種類のレンダリング・アプリケーション34を実行することを決定することができる。例えば、ファイル名拡張子が、デジタル・コンテ

ンツ12はテキスト・ファイルであることを示す場合、レンダリング・アプリケーション34は、ワシントン州RedmondのMICROSOFT Corporationが販売する“MICROSOFT WORD”のようなワード・プロセッサの何らかの形態となる。同様に、ファイル名拡張子が、デジタル・コンテンツ12はオーディオ、ビデオ、および/またはマルチメディア・ファイルであることを示す場合、レンダリング・アプリケーション34は、同様にワシントン州RedmondのMICROSOFT Corporationが販売する“MICROSOFT MEDIA PLAYER”のような、マルチメディア・プレーヤの何らかの形態となる。

【0058】

勿論、レンダリング・アプリケーションを決定する他の方法も採用することができ、本発明の精神および範囲から逸脱する訳ではない。一例としてに過ぎないが、デジタル・コンテンツ12は、無暗号化形態のメタデータ（前述のヘッダ情報）を含むこともでき、この場合、メタデータは、このようなデジタル・コンテンツ12をレンダリングするために必要なレンダリング・アプリケーション34の形式に関する情報を含む。

【0059】

好ましくは、このようなレンダリング・アプリケーション34は、ファイル名に関連するデジタル・コンテンツ12を試験し、このようなデジタル・コンテンツ12が権利保護形態で暗号化されているか否か判定を行なう（ステップ503，505）。保護されていない場合、これ以上の面倒なく、デジタル・コンテンツ12をレンダリングすることができる（ステップ507）。保護されている場合、レンダリング・アプリケーション34は、暗号化デジタル・コンテンツ12から、このようなデジタル・コンテンツ12を再生するためにDRMシステム32が必要か否か判定を行なう。これに応じて、このようなレンダリング・アプリケーション34は、ユーザの計算機14に、DRMシステム32をその上で走らせるように指令する（ステップ509）。次に、このようなレンダリング・アプリケーション34はこのようなDRMシステム32をコールし、デジタル・コンテンツ12を解読する（ステップ511）。以下で更に詳しく論ずるが、DRMシステム32は、実際には、ユーザがこのようなデジタル・コンテンツ12に対

する有効なライセンス16、および有効なライセンス16におけるライセンス規則にしたがってデジタル・コンテンツ12を再生する権利を有する場合にのみ、デジタル・コンテンツ12を解読する。好ましくは、一旦DRMシステム32がレンダリング・アプリケーション34によってコールされた場合、このようなDRMシステム32は、少なくとも、ユーザがこのようなデジタル・コンテンツ12を再生する権利を有するか否か判定を行なう目的で、レンダリング・アプリケーション34から制御を引き受ける（ステップ513）。

DRMシステム32のコンポーネント

ライセンス評価部36は、要求されたデジタル・コンテンツ12に対応する1つ以上のライセンス16を突き止め、このようなライセンス16が有効であるか否か判定を行い、このような有効なライセンス16におけるライセンス規則を見直し、見直したライセンス規則に基づいて、要求元のユーザが、とりわけ、求められた状態で、要求したデジタル・コンテンツ12をレンダリングする権利を有するか否か判定を行なう。当然理解されようが、ライセンス評価部36は、DRMシステム32における信頼コンポーネント（trusted component）である。この開示では、「信頼」とは、信頼エレメントが、ライセンス16における権利の記述にしたがってデジタル・コンテンツ12の所有者の望みを遂行することをライセンス・サーバ24（またはその他のあらゆる信頼する側のエレメント（trusting element））に納得させること、およびユーザがいずれの邪悪なまたはその他の目的のためにもこのような信頼エレメントを容易に変更できないことを意味する。

【0060】

ライセンス評価部36が実際にライセンス16を適性に評価することを保証するため、そしてこのようなライセンス評価部36が、ライセンス16の実際の評価を迂回する目的でユーザが偽造またはそれ以外に変更されていないことを保証するために、このようなライセンス評価部36は信頼されなければならない。したがって、ライセンス評価部36は、保護または隠蔽された環境で走り、このようなライセンス評価部36へのユーザのアクセスが拒否されるようにする。勿論、その他の保護対策も、ライセンス評価部36に関して採用することができ、本

発明の精神および範囲から逸脱することはない。

DRMシステム32のコンポーネント—ブラック・ボックス30

主に、そして先に論じたように、ブラック・ボックス30は、DRMシステム32において暗号化および解読機能を実行する。即ち、ブラック・ボックス30は、ライセンス評価部36と共に動作し、ある情報をライセンス評価機能の一部として解読および暗号化する。加えて、一旦ライセンス評価部36が、実際にユーザが求められた態様で要求デジタル・コンテンツ12をレンダリングする権利を有すると判定したなら、ブラック・ボックス30には、このようなデジタル・コンテンツ12のために解読鍵(KD)が与えられ、このような解読鍵(KD)に基づいて、このようなデジタル・コンテンツ12を解読する機能を実行する。

【0061】

また、ブラック・ボックス30もDRMシステム32における信頼コンポーネントである。即ち、ライセンス・サーバ24は、ブラック・ボックス30が、ライセンス16におけるライセンス規則にしたがってのみ解読機能を実行することを信用しなければならず、更にライセンス16の実際の評価を迂回するという邪悪な目的でユーザによって偽造またはそれ以外に変更された場合には、このようなブラック・ボックス30は動作しないことも信用しなければならない。したがって、ブラック・ボックス30も保護即ち隠蔽された環境で走り、ユーザはこのようなブラック・ボックス30へのアクセスを拒否される。この場合も、ブラック・ボックス30に関して他の保護対策を採用することもでき、本発明の精神および範囲から逸脱することはない。好ましくは、そしてコンテンツ・サーバ22およびライセンス・サーバ24と同様に、DRMシステム32におけるブラック・ボックス30は、一意の公開／秘密鍵対(PU-BB, PR-BB)を有し、ライセンス16を評価し、デジタル・コンテンツ12を解読するための解読鍵(KD)を取得するプロセスの一部として用いられる。これについては、以下で更に詳しく説明する。

DRMシステム32のコンポーネント—ライセンス・ストア38

ライセンス・ストア38は、DRMシステム32が対応するデジタル・コンテンツ12に対して受領したライセンス16を格納する。ライセンス・ストア38

自体は、信頼される必要はない。何故なら、ライセンス・ストア38は単にライセンス16を格納するだけに過ぎず、その各々は既に信頼コンポーネントとして組み込まれているからである。これについては以下で説明する。本発明の一実施形態では、ライセンス・ストア38は、単に、ハード・ディスク・ドライブまたはネットワーク・ドライブのようなドライブのサブディレクトリである。しかしながら、ライセンス・ストア38は、DRMシステム32に比較的好都合な場所においてライセンス16を格納する機能を実行する限りにおいて、本発明の精神および範囲から逸脱することなく、他のあらゆる形態で具体化することも可能である。

DRMシステム32のコンポーネント—状態ストア40

状態ストア40は、現在または以前ライセンス・ストア38にあったライセンス38に対応する状態情報を維持する機能を実行する。このような状態情報は、DRMシステム32が作成し、必要に応じて状態ストア40に格納される。例えば、特定のライセンス16が対応する1片のデジタル・コンテンツ12の所定回数のレンダリングのみを許可する場合、状態ストア40は、このようなライセンス16に関して実際にレンダリングが何回行われたかに関する状態情報を維持する。状態ストア40は、もはやライセンス・ストア38にはないライセンス16に関する状態情報を維持し続け、状態ストア40から対応する状態ストア情報を削除する試みにおいて、ライセンス・ストア38からライセンス16を削除し、次いで同じライセンス16を取得することが有利となるような状況を回避する。

【0062】

また、状態ストア40も、内部に格納されている情報が、ユーザに一層好ましい状態にはリセットされないことを保証するために、信頼されなければならない。したがって、状態ストア40も同様に保護即ち隠蔽された環境で走り、このような状態ストア40に対するユーザのアクセスが拒否されるようにする。この場合も、状態ストア40に関して他の保護対策を勿論採用することができ、本発明の精神および範囲から逸脱することはない。例えば、状態ストア40は、DRMシステム32によって、暗号化形態で計算機14上に格納してもよい。

DRMシステム32—コンテンツ・レンダリング、第2部

再度図5Aを参照し、本発明の一実施形態におけるコンテンツ・レンダリングについて再度論ずる。一旦DRMシステム32が、コール元のレンダリング・アプリケーション34から制御を引き受けたなら、このようなDRMシステム32は、ユーザが求められた状態で要求されたデジタル・コンテンツ12をレンダリングする権利を有するか否か判定を行なうプロセスを開始する。即ち、DRMシステム32は、ライセンス・ストアにおいて有効な授権ライセンス16を突き止めるか（ステップ515、517）、あるいはライセンス・サーバ24から有効な授権ライセンス（enabling license）16を取得しようとする（即ち、以下で論じ図7に示すライセンス取得機能を実行する）。

【0063】

第1ステップとして、そしてここで図6を参照して、このようなDRMシステム32のライセンス評価部36は、ライセンス38をチェックして、デジタル・コンテンツ12に対応する1つ以上のライセンス16を受信しているか否か確認する（ステップ601）。典型的に、ライセンス16は、以下で論ずるように、デジタル・ファイルの形態となっているが、本発明の精神および範囲から逸脱することなくライセンス16は他の形態でもよいことは認められよう。典型的に、ユーザは、このようなライセンス16がなくてもデジタル・コンテンツ12を受信するが、本発明の精神および範囲から逸脱することなく、対応するライセンス16と共に、デジタル・コンテンツ12を受信するようにしてもよいことも同様に認められよう。

【0064】

図3に関連付けて先に論じたように、デジタル・コンテンツ12の各片は、パッケージ12p内にあり、コンテンツID（またはパッケージID）がこのようなデジタル・コンテンツ12（またはパッケージ12p）を識別し、鍵IDが、暗号化デジタル・コンテンツ12を解読する解読鍵（KD）を識別する。好ましくは、コンテンツID（またはパッケージID）および鍵IDは、無暗号化形態である。したがって、そして具体的には、デジタル・コンテンツ12のコンテンツIDに基づいて、ライセンス評価部36は、このようなコンテンツIDの適用可能性の識別を収容するライセンス・ストア8において、あらゆるライセンス1

6を探す。尚、特にデジタル・コンテンツ12の所有者がこのようなデジタル・コンテンツ12に対して数種類の異なるライセンス16を有し、ユーザがこのようなライセンス16を多数個取得している場合、このようなライセンス16が多数見つかる場合もあることを注記しておく。実際に、ライセンス評価部36がライセンス・ストア38において、要求されたデジタル・コンテンツ12に対応するライセンス16を全く発見できない場合、DRMシステム32は、以下で説明するライセンス取得機能を実行する(図5のステップ519)。

【0065】

ここで、DRMシステム32が、1枚のデジタル・コンテンツ12をレンダリングするように要求されており、対応する1つ以上のライセンス16がライセンス・ストア38内にあると仮定する。本発明の一実施形態では、ここで、DRMシステム32のライセンス評価部36は続いて、このようなライセンス16の各々について、このようなライセンス16自体が有効か否か判定する(図6のステップ603および605)。好ましくは、そして具体的に、各ライセンス116は、当該ライセンス16の内容28に基づいたデジタル署名26を含む。当然理解されようが、デジタル署名26は、コンテンツ28が偽造またはそれ以外に変更されている場合、ライセンス16とは一致しない。したがって、ライセンス評価部36は、デジタル署名26に基づいて、コンテンツ28が、ライセンス・サーバ24から受け取った形態になっているか(即ち、有効か)否か、判定を行なうことができる。ライセンス・ストア38において有効なライセンス16が見つからない場合、DRMシステム32は、以下で説明するライセンス取得機能を実行し、このような有効なライセンス16を取得することができる。

【0066】

1つ以上の有効なライセンス16が見つかったと仮定すると、有効なライセンス16各々について、DRMシステム32のライセンス評価部36は、次に、このような有効なライセンス16が、望ましい態様で対応するデジタル・コンテンツ12をレンダリングする権利をユーザに与えるか(即ち、授權するか)否か判定を行なう。即ち、ライセンス評価部36は、要求元のユーザが要求したデジタル・コンテンツ12を再生する権利を有するか否か、各ライセンス16における

権利の記述に基づいて、更にユーザがデジタル・コンテンツ12で何をしようとしているのかに基づいて判定を行なう。例えば、このような権利の記述は、ユーザに、デジタル・コンテンツ12をサウンドにレンダリングすることは許可するが、解読してデジタル・コピーにレンダリングすることは許可しない。

【0067】

当然理解されようが、各ライセンス16における権利の記述は、いくつかの要因のいずれかに基づいて、ユーザがデジタル・コンテンツ12を再生する権利を有するか否か指定する。要因には、ユーザが誰であるか、ユーザがどこにいるか、どの種類の計算機114をユーザが用いているか、どのレンダリング・アプリケーション34がDRMシステム32をコールしているのか、日付、時間等が含まれる。加えて、権利の記述は、例えば、所定回数の再生、所定の再生時間にライセンス16を限定することもできる。このような場合、DRMシステム32は、ライセンス16に関するあらゆる状態情報を参照しなければならない（即ち、何回デジタル・コンテンツ12がレンダリングされたか、デジタル・コンテンツ12がレンダリングされた総時間量等）。このような状態情報は、ユーザの計算機14のDRMシステム32の状態ストア40に格納されている。

【0068】

したがって、DRMシステム32のライセンス評価部36は、有効な各ライセンス16の権利の記述を検討し、このような有効なライセンス16が、ユーザに求められた権利を授与するか否か判定を行なう。これを行なう際、ライセンス評価部36は、ユーザの計算機14内部の別のデータを参照して、ユーザが求めた権利を有するか否かの判定を実行しなければならない場合もある。図4に見られるように、このようなデータは、ユーザの計算機（機械）14の識別42およびその特定の態様、ユーザの識別44およびその特定の態様、レンダリング・アプリケーション34の識別およびその特定の態様、システム・クロック46等を含むことができる。ユーザに求められた態様でデジタル・コンテンツ12をレンダリングする権利を与える有効なライセンス16が見つからない場合、DRMシステム32は、次に、以下で説明するライセンス取得機能を実行し、実際にこのようなライセンス16が取得可能であれば、このようなライセンス16を取得

する。

【0069】

勿論、場合によっては、ユーザは要求した態様でデジタル・コンテンツ12をレンダリングする権利を取得できないこともある。何故なら、このようなデジタル・コンテンツ12のコンテンツ所有者は、ユーザにテキスト文書を印刷したり、マルチメディア表現を無暗号化形態にコピーすることを許可するライセンス16を付与しないことを指令している場合もあるからである。本発明の一実施形態では、デジタル・コンテンツ12は、ライセンス16の購入時にどんな権利が利用可能かに関するデータ、および利用可能なライセンス16の種類を含む。しかしながら、1片のデジタル・コンテンツ12のコンテンツ所有者は、いずれの時点においても、このようなデジタル・コンテンツ12に対して得られるライセンス16を変更することによって、このようなデジタル・コンテンツ12に現在利用可能な権利を変更する可能性があることは認められよう。

DRMシステム32—ライセンス取得

ここで図7を参照すると、実際にライセンス評価部36がライセンス・ストア38において、要求されたデジタル・コンテンツ12に対応する有効な授權ライセンス16を全く見つけられない場合、DRMシステム32は、ライセンス取得機能を実行する。図3に示すように、デジタル・コンテンツ12の各片は、このようなデジタル・コンテンツ12をレンダリングするためのライセンス16を取得するにはどうすればよいかに関する無暗号化形態の情報（即ち、ライセンス取得情報）と共にパッケージ化されている。

【0070】

本発明の一実施形態では、このようなライセンス取得情報は、利用可能なライセンス16の種類、および1つ以上の適切なライセンス・サーバ24にアクセスすることができる1つ以上のインターネット・ウェブ・サイトまたはその他のサイト情報を（とりわけ）含むことができる。ここで、各ライセンス・サーバ24は実際にデジタル・コンテンツ12に対応するライセンス16を発行することができる。勿論、ライセンスは、他の態様で取得することもでき、本発明の精神および範囲から逸脱する訳ではない。例えば、ライセンス16は、電子掲示板にお

いてライセンス・サーバ24から取得したり、あるいは自分自身でまたは磁気または光ディスク等のファイルという形態で正規のメールによって取得することもできる。

【0071】

ライセンス16を取得するための場所が、実際にネットワーク上のライセンス・サーバ24であると仮定すると、ライセンス評価部36は、ウェブ・サイトまたはその他のサイト情報に基づいてこのようなライセンス・サーバ24に対してネットワーク接続を確立し、次いでこのように接続したライセンス・サーバ24からライセンス16の要求を送る（ステップ701、703）。即ち、一旦DRMシステム32がライセンス・サーバ24とコンタクトしたなら、このようなDRMシステム32は適切なライセンス要求情報37をこのようなライセンス・サーバ24に送信する。本発明の一実施形態では、このようなライセンス16の要求情報36は、とりわけ、次を含むことができる。

【0072】

- DRMシステム32のブラック・ボックス30の公開鍵（PU-BB）、
- DRMシステム32のブラック・ボックス30のバージョン番号、
- ブラック・ボックス30を認証した証明機関からのデジタル署名を含む認証書（認証書は実際に前述のブラック・ボックス30の公開鍵およびバージョン番号を含むこともできる）、
- デジタル・コンテンツ12（またはパッケージ12p）を識別するコンテンツID（またはパッケージID）、
- デジタル・コンテンツ12を解読するための解読鍵（KD）を識別する鍵ID、
- 要求されたライセンス16の種類（実際に多数の種類が使用可能な場合）、
- デジタル・コンテンツ12のレンダリングを要求したレンダリング・アプリケーション34の種類等。

【0073】

勿論、これらよりも多い量または少ない量のライセンス16の要求情報36を、DRMシステム32によって、ライセンス・サーバ24に送信することもでき

、本発明の精神および範囲から逸脱することはない。例えば、レンタル・アプリケーション34の種類に関する情報が必要ではない場合もあり、一方ユーザおよび/またはユーザの計算機14に関して追加の情報が必要な場合もある。

【0074】

一旦ライセンス・サーバ24がDRMシステム32からライセンス16の要求情報36を受信したなら、ライセンス・サーバ24は、信頼/認証およびその他の目的のために、いくつかのチェックを行なうとよい。本発明の一実施形態では、このようなライセンス・サーバ24は、証明機関のデジタル署名を含む認証書をチェックし、これが偽造またはそれ以外に変更されていないか否か判定を行なう(ステップ705、707)。されている場合、ライセンス・サーバ24は、要求情報36に基づいてあらゆるライセンス16を付与することを拒否する。また、ライセンス・サーバ24は、判明した「悪い」ユーザおよび/またはユーザの計算機14のリストを保持することもでき、更にリスト上にあるこのような悪いユーザおよび/または悪いユーザの計算機14からの要求に基づいて、あらゆるライセンス16を付与するのを拒否することもできる。このような「悪人」リストは、いずれの適切な態様でもコンパイルすることができ、本発明の精神および範囲から逸脱することはない。

【0075】

受信した要求およびそれに付随する情報に基づいて、特にライセンス要求情報におけるコンテンツID(またはパッケージID)に基づいて、ライセンス・サーバ24はコンテンツ鍵データベース20(図1)に問い合わせ、要求の基準であるデジタル・コンテンツ12(またはパッケージ12p)に対応するレコードを突き止める。先に論じたように、このようなレコードは、このようなデジタル・コンテンツ12に対する解読鍵(KD)、鍵ID、およびコンテンツIDを含む。加えて、このようなレコードは、デジタル・コンテンツ12に発行するライセンス16の種類、ならびにライセンス16の各種類毎の条件に関するライセンス・データを収容することができる。あるいは、このようなレコードは、このような追加情報を有する場所へのポインタ、リンク、または参照を含むこともできる。

【0076】

前述のように、多数の種類のライセンス16を得ることができる。例えば、比較的小額のライセンス料では、限られた回数のレンダリングを許可するライセンス16を得ることができる。比較的大きな額のライセンス料では、満期日まで無制限のレンダリングを許可するライセンス16を得ることができる。更に高額のライセンス料では、満期日なしで無制限のレンダリングを許可するライセンスを得ることができる。実際には、あらゆる種類のライセンス条件を有するあらゆる種類のライセンス16でも、ライセンス・サーバ24によって考案し発行することもでき、本発明の精神および範囲から逸脱することはない。

【0077】

本発明の一実施形態では、ライセンス16の要求は、ライセンス・サーバ24からユーザの計算機14まで送信する際に、ウェブ・ページ等の助けによって行われる。好ましくは、このようなウェブ・ページは、ライセンス16の要求の基準であるデジタル・コンテンツ12に対してライセンス・サーバ24から得られるあらゆる種類のライセンス16に関する情報を含む。

【0078】

本発明の一実施形態では、ライセンス16を発行するのに先立って、ライセンス・サーバ24は、ブラック・ボックス30のバージョン番号をチェックし、このようなブラック・ボックス30が比較的新しいか否か判定を行なう（ステップ709、711）。当然理解されようが、ブラック・ボックス30は、安全であり、邪悪な目的（即ち、ライセンス16なく不適正にデジタル・コンテンツ12をレンダリングしたり、対応するライセンス16の条件に外れている）のユーザからの攻撃から保護することを目的とする。しかしながら、実際にはこのような攻撃から完全に安全なシステムもソフトウェアもないことは認められよう。

【0079】

当然理解されようが、ブラック・ボックス30が比較的新しい場合、即ち、比較的最近取得または更新された場合、このようなブラック・ボックス30がこのような邪悪なユーザによる攻撃を受けて成功する可能性は少ない。好ましくは、そして信頼問題として、ライセンス・サーバ24が、比較的新しくないブラック

・ボックス30のバージョン番号を含む要求情報を有するライセンス要求を受信した場合、このようなライセンス・サーバ24は、対応するブラック・ボックス30が現行バージョンにアップグレードされるまで、要求されたライセンス16を発行することを拒否する。これについては以下で説明する。単純に言えば、ライセンス・サーバ24は、このようなブラック・ボックス30が比較的新しくなければ、このようなブラック・ボックス30を信頼しない。

【0080】

本発明のブラック・ボックス30に関連して、「新しい」または「比較的新しい」という用語は、ブラック・ボックス30の使用年数および利用度に基づいてブラック・ボックス30に信頼を与える機能と一貫して、適切な意味を有することができ、本発明の精神および範囲から逸脱することはない。例えば、「新しい」は、年数にしたがって定義することができる（即ち、1か月未満）。別の例として、「新しい」は、ブラックボックス30がデジタル・コンテンツを解読した回数に基づいて定義することもできる（即ち、解読が200回未満）。更に、「新しい」は、各ライセンス・サーバ24が設定する理念に基づくこともでき、この場合1つのライセンス・サーバ24は別のライセンス・サーバとは異なる定義を「新しい」に対してすることもでき、更に、とりわけ、ライセンス16が要求されるデジタル・コンテンツ12に応じて、または要求されたライセンス16の種類に応じて、ライセンス・サーバ24は「新しい」を別個に定義することもできる。

【0081】

ブラック・ボックス30のバージョン番号またはこのようなブラック・ボックス30のその他の指標が新しいことに、ライセンス・サーバ24が納得したと仮定すると、ライセンス・サーバ24は次にユーザとライセンス16の条件を交渉する。あるいは、ライセンス・サーバ24はユーザとライセンス16の交渉を行い、このようなブラック・ボックス30が新しいことを示すブラック・ボックス30のバージョン番号にそれ自体が納得する（ステップ713、次いで711を実行する）。勿論、交渉の量は、発行するライセンス16の種類、およびその他の要因によって異なる。例えば、ライセンス・サーバ24が単に一括払い無制限

使用ライセンス16を発行する場合、殆ど交渉を行なう必要はない。一方、ライセンス16が、変動する価値、スライド制、区切り点、およびその他の詳細のような項目に基づく場合、このような項目および詳細は、ライセンス・サーバ24およびユーザ間で、ライセンス16を発行可能となる前に案出しなければならない場合もある。

【0082】

当然理解されようが、状況によっては、ライセンスの交渉は、ユーザが更にライセンス・サーバ24に情報を提供しなければならないこともあり得る（例えば、ユーザ、ユーザの計算機14等に関する情報）。重要なことは、ライセンスの交渉は、とりわけ、ユーザおよびライセンス・サーバ24が相互に受諾可能な支払手段（クレジット・アカウント、デビット・アカウント、郵送による小切手等）および／または支払方法（即時一括払い、ある時間期間の分割）を決定しなければならないことである。

【0083】

一旦ライセンス16の全ての条件について交渉を行い、ライセンス・サーバ24およびユーザ双方が同意したなら（ステップ715）、ライセンス・サーバ24がデジタル・ライセンス16を生成する（ステップ719）。このように生成するライセンス16は、少なくとも部分的に、ライセンス要求、ブラック・ボックス30の公開鍵（PU-BB）、およびコンテンツ鍵データベース20から取得した要求の基準となるデジタル・コンテンツ12に対する解読鍵（KD）に基づいている。本発明の一実施形態では、そして図8に見られるように、生成したライセンス16は次を含む。

【0084】

ーライセンス16を適用するデジタル・コンテンツ12のコンテンツID、
ー恐らくは解読鍵（KD）（即ち、KD（DRL））で暗号化されている、デジタル権利ライセンス（DRL）48（即ち、ライセンス評価部36が問い合わせることができる所定の書式で書かれたライセンス16の権利の記述即ち実際の条件）、

ーライセンス要求において受信したブラック・ボックス30の公開鍵（PU-

BB)で暗号化したデジタル・コンテンツ12に対する解読鍵(KD)(即ち(PU-BB(KD)))。

【0085】

ー(KD(DRL))および(PU-BB(KD))に基づき、ライセンス・サーバ24の秘密鍵(即ち、(S(PR-LS)))を用いて暗号化した、ライセンス・サーバ24からのデジタル署名(認証書の添付なし)、および

ーライセンス・サーバ24がコンテンツ・サーバ22から以前に取得した認証書。このような認証書は、ライセンス・サーバ24がコンテンツ・サーバ22からのライセンス16を発行する権限を有することを示す(即ち、(CERT(PU-LS)S(PR-CS)))。

【0086】

当然理解されようが、前述のエレメントおよび恐らくその他のエレメントも、デジタル・ファイルまたはその他の何らかの適切な形態にパッケージ化される。同様に当然理解されようが、DRL48またはライセンス16における(PU-BB(KD))が偽造またはそれ以外に変更されている場合、ライセンス16におけるデジタル署名(S(PR-LS))は一致せず、したがって、このようなライセンス16は有効性が認められない。この理由のため、DRLは必ずしも前述のような暗号化形態(即ち、(KD(DRL)))である必要はないが、場合によってはこのような暗号化形態が望ましい場合もあり、したがって、本発明の精神および範囲から逸脱することなく、採用してもよい。

【0087】

一旦デジタル・ライセンス16の準備が終了すると、次にこのようなライセンス16を要求元(即ち、ユーザの計算機14上のDRMシステム32)(図7のステップ719)。好ましくは、ライセンス16は、その要求が行われたのと同じ経路(即ち、インターネットまたはその他のネットワーク)を通じて送信するといいが、他の経路を用いてもよく、本発明の精神および範囲から逸脱することはない。受信時に、要求元DRM32は、自動的に受信したデジタル・ライセンス16をライセンス・ストア38に置くことが好ましい(ステップ721)。

【0088】

尚、ユーザの計算機14は、場合によっては誤動作する場合もあり、このようなユーザの計算機14上のDRMシステム32のライセンス・ストア38に格納されているライセンス16が検索不能となり、失われる場合もあり得ることは理解されよう。したがって、ライセンス・サーバ24は、発行したライセンス16のデータベース50(図1)を保持し、ユーザに実際に再発行を受ける権利がある場合、このようなライセンス・サーバ25が、ユーザに発行したライセンス16のコピーを与えるかまたは再発行を行なう(以後、「再発行」)ようにすることが好ましい。ライセンス16が検索不能となり失われるという前述の場合では、状態ストア40に格納されており、このようなライセンス16に対応する状態情報も失われる可能性もある。このように失われた状態情報は、ライセンス16を再発行する際に考慮に入れなければならない。例えば、比較的短い時間期間の後に一定の割合に応じた形態で固定数のレンダリング・ライセンス16を合法的に再発行し、比較的長い時間期間の後には全く再発行しないことも可能である。

DRMシステム32—ブラック・ボックス30のインストール／更新

先に論じたように、ライセンス16を取得する機能の一部として、ライセンス・サーバ24は、ユーザの計算機14のDRMシステム32が、比較的新しくないブラック・ボックス30、即ち、比較的古いバージョン番号を有するブラック・ボックス30を有する場合、ユーザからのライセンス16の要求を拒否することができる。このような場合、このようなDRMシステム32のブラック・ボックス30を更新し、ライセンス取得機能が進行できるようにすることが好ましい。勿論、ブラック・ボックス30は他の時点でも更新可能であり、本発明の精神および範囲から逸脱することはない。

【0089】

好ましくは、ユーザの計算機14上にDRMシステム32をインストールするプロセスの一部として、ブラック・ボックス30の一意でない「ライト」(lite)バージョンを用意する。このような「ライト」ブラック・ボックス30は、1片のデジタル・コンテンツ12をレンダリングする前に、一意の正規バージョンにアップグレードする。当然理解されようが、各DRMシステム32における各ブラック・ボックス30が一意であれば、1つのブラック・ボックス30へのセ

セキュリティ侵害は、他のいずれのブラック・ボックス30に対しても容易に繰り返すことはできない。

【0090】

次に図9を参照すると、DRMシステム32は、ブラック・ボックス・サーバ等から要求することによって、一意のブラック・ボックス30を取得する（先に論じ、図1に示した通りである）（ステップ901）。典型的に、このような要求を行なうにはインターネットを用いるが、他のアクセス手段も採用でき、本発明の精神および範囲から逸脱することはない。例えば、ブラック・ボックス・サーバ26への接続は、ローカルまたはリモートのいずれでも、直接接続とすることができる。1つの一意の非ライト・ブラック・ボックス30から別の一意の非ライト・ブラック・ボックス30へのアップグレードも、いずれの時点においても、例えば、ライセンス・サーバ24がブラック・ボックス30を新しくないと見なしたときのように、DRMシステム32によって要求することができる。これは、先に論じた通りである。

【0091】

その後、ブラック・ボックス・サーバ26は、新たな一意のブラック・ボックス30を生成する（ステップ903）。図3に見られるように、新たなブラック・ボックス30の各々には、バージョン番号、および証明機関からのデジタル署名を有する認証書が備えられている。ライセンス取得機能との関連で先に論じたように、ブラック・ボックス30のバージョン番号は、その相対的な使用期間（age）および／または使用を示す。同様にライセンス取得機能との関連で先に論じた、証明機関からのデジタル署名を有する認証書は、ライセンス・サーバ24がブラック・ボックス30を信頼するという、証明機関からの申し出即ち証拠機構である。勿論、ライセンス・サーバ24は、証明機関がこのような認証書を、実際に信頼のおけるブラック・ボックス30に発行することを信用する。実際には、ライセンス・サーバ24が特定の証明機関を信頼せず、このような証明機関が発行するいずれの認証書も有効と認めることを拒絶する場合もあり得る。例えば、特定の証明機関が不正に認証書を発行しているパターンに関与していることが発覚した場合、信頼を得ることはできない。

【0092】

好ましくは、そして先に論じたように、ブラック・ボックス・サーバ26は、新たに生成した一意のブラック・ボックス30を有する新たな一意の公開／秘密鍵対(PU-BB, PR-BB)を含む。好ましくは、ブラック・ボックス30の秘密鍵(PU-BB)は、このようなブラック・ボックス30のみからアクセス可能であり、このようなブラック・ボックス30を含むDRMシステム32を有する計算機14およびそのユーザを含めて、世界のその他からは隠されており、アクセスすることはできない。

【0093】

あらゆる秘匿方式は、実際にこのような秘匿方式が世界から秘密鍵(PU-BB)を隠す機能を実行する限り、その殆どを用いることができ、本発明の精神および範囲から逸脱することはない。一例としてに過ぎないが、秘密鍵(PU-BB)をいくつかのサブコンポーネントに分割し、各サブコンポーネントを一意に暗号化し、異なる場所に格納してもよい。このような状況では、このようなサブアセンブリを完全に組み立てて完全な秘密鍵(PU-BB)を決して生成しないことが好ましい。

【0094】

本発明の一実施形態では、このような秘密鍵(PU-BB)を暗号化するには、コードを用いる暗号化技術に従う。即ち、このような実施形態では、ブラック・ボックス30の実際のソフトウェア・コード(または他のソフトウェア・コード)が暗号化鍵(複数の暗号化鍵)として用いられる。したがって、例えば、邪悪な目的でユーザによってブラック・ボックス30のコード(またはその他のソフトウェア・コード)が偽造されたり、あるいは他の方法で変更された場合、このような秘密鍵(PU-BB)を解読することはできない。

【0095】

新たなブラック・ボックス30の各々は、新たな公開／秘密鍵対(PU-BB, PR-BB)と共に配信されるが、このような新たなブラック・ボックス30には、ユーザの計算機14上のDRMシステム32に以前に配信した古いブラック・ボックス30からの古い公開／秘密鍵対へのアクセスも与えることが好まし

い（ステップ905）。したがって、アップグレードしたブラック・ボックス30は、古い鍵対を用いて、古いデジタル・コンテンツ12およびこのような古い鍵対にしたがって生成した、対応する古いライセンス16にもアクセスすることができる。これについては、以下で更に詳しく論ずる。

【0096】

好ましくは、ブラック・ボックス・サーバ26が配信するアップグレードしたブラック・ボックス30は、ユーザの計算機14に密接に連結即ち関連付けられる。したがって、アップグレードしたブラック・ボックス30は、邪悪な目的およびその他のために、多数の計算機間で動作可能に転送することはできない。本発明の一実施形態では、ブラック・ボックス30の要求（ステップ901）の一部として、DRMシステム32は、このようなDRMシステム32に一意の、および／またはユーザの計算機14に一意のハードウェア情報を、ブラック・ボックス・サーバ26に提供し、ブラック・ボックス・サーバ26は、部分的にこのような提供されたハードウェア情報に基づいて、DRMシステム32にブラック・ボックス30を生成する。このように生成されたアップグレード・ブラック・ボックス30は、次にユーザの計算機14に配信され、DRMシステム32にインストールされる（ステップ907、909）。アップグレードしたブラック・ボックス30が何らかの方法で別の計算機14に転送された場合、転送されたブラック・ボックス30は、このような他の計算機14を対象とするのではないことを認識し、このようなその他の計算機14上でレンダリングを進める要求を全て許可しない。

【0097】

一旦新たなブラック・ボックス30がDRMシステム32にインストールされると、このようなDRMシステム32は、ライセンス取得機能またはその他のいずれかの機能を実行することができる。

DRMシステム32—コンテンツ・レンダリング、第3部

次に図5Bを参照し、ここでライセンス評価部36が少なくとも1つの有効なライセンス16を発見し、このような有効なライセンス16の少なくとも1つが、求められた態様で対応するデジタル・コンテンツ12をレンダリングするため

に必要な権利（即ち、授權）をユーザに与えることがわかったと仮定すると、ライセンス評価部36は、更に用いるためにこのようなライセンス16の1つを選択する（ステップ519）。即ち、要求されたデジタル・コンテンツ12をレンダリングするために、ライセンス評価部36およびブラック・ボックス30は、一体となってこのようなライセンス16から解読鍵（KD）を取得し、ブラック・ボックス30はこのような解読鍵（KD）を用いて、デジタル・コンテンツ12を解読する。本発明の一実施形態では、そして先に論じたように、ライセンス16から取得した解読鍵（KD）は、ブラック・ボックス30の公開鍵（PUBB（KD））で暗号化されており、ブラック・ボックス30は、その秘密鍵（PUBB）を用いて、このように暗号化されている解読鍵を解読し、解読鍵（KD）を生成する（ステップ521、523）。しかしながら、デジタル・コンテンツ12の解読鍵（KD）を取得するその他の方法を用いてもよく、本発明の精神および範囲から逸脱することはない。

【0098】

一旦ブラック・ボックス30がデジタル・コンテンツ12の解読鍵（KD）を有し、ライセンス評価部36からデジタル・コンテンツ12をレンダリングする許可を得たなら、制御をレンダリング・アプリケーション34に戻すことができる（ステップ525、527）。本発明の一実施形態では、レンダリング・アプリケーション34は次にDRMシステム32／ブラック・ボックス30をコールし、暗号化デジタル・コンテンツ12の少なくとも一部をブラック・ボックス30に送出し、解読鍵（KD）にしたがって解読する（ステップ529）。ブラック・ボックス30は、デジタル・コンテンツ12の解読鍵（KD）に基づいてデジタル・コンテンツ12を解読し、次いでブラック・ボックス30は、解読したデジタル・コンテンツ12を実際にレンダリングするために、レンダリング・アプリケーション34に戻す（ステップ533、535）。レンダリング・アプリケーション34は、暗号化デジタル・コンテンツ12の一部またはデジタル・コンテンツ12全体をブラック・ボックス30に送り、本発明の精神および範囲から逸脱することなく、このようなデジタル・コンテンツ12の解読鍵（KD）に基づいて解読することができる。

【0099】

好ましくは、レンダリング・アプリケーション34がデジタル・コンテンツ12をブラック・ボックス30に送り解読する場合、ブラック・ボックス30および/またはDRMシステム32はこのようなレンダリング・アプリケーション34の認証を行い、これが実際にDRMシステム32に最初に走らせるように要求したのと同じレンダリング・アプリケーションであることを確認する（ステップ531）。あるいは、レンダリングの承認が、ある種のレンダリング・アプリケーション34に対するレンダリング要求に基づき、実際に他の種類のレンダリング・アプリケーション34でレンダリングすることによって、不正に取得されたという可能性もあり得る。認証に成功し、デジタル・コンテンツ12がブラック・ボックス30によって解読されたと仮定すると、レンダリング・アプリケーション34は解読されたデジタル・コンテンツ12をレンダリングすることができる（ステップ533、535）。

鍵トランザクション・シーケンス

次に図10を参照すると、本発明の一実施形態では、鍵トランザクション・シーケンスを実行して、要求された1片のデジタル・コンテンツ12に対する解読鍵（KD）を取得し、ライセンス16を評価する（即ち、図5Aおよび図5Bのステップ515ないし523を実行する）。このシーケンスでは、主にDRMシステム32はライセンス16から解読鍵（KD）を取得し、ライセンス16およびデジタル・コンテンツ12から得た情報を用いて、双方の有効性を認証即ち確認し、次いでライセンス16が実際に求められた態様でデジタル・コンテンツ12をレンダリングする権利を与えるか否か判定を行なう。与える場合、デジタル・コンテンツ12をレンダリングすることができる。

【0100】

図8に示すように、デジタル・コンテンツ12の各ライセンス16が次を含むことを念頭に入れ、

- ライセンス16を適用するデジタル・コンテンツ12のコンテンツID、
- 恐らく解読鍵（KD）で暗号化されているデジタル権利ライセンス（DRL）48（即ち、KD（DRK））。

【0101】

—ブラック・ボックス30の公開鍵(PU-BB)で暗号化されているデジタル・コンテンツ12の解読鍵(KD)(即ち、(PU-BB(KD))、

—(KD(DRK))および(PU-BB(KD))に基づいて、そしてライセンス・サーバ24の秘密鍵で暗号化されている、ライセンス・サーバ24からのデジタル署名(即ち、(S(PR-LS)))、および

—ライセンス・サーバ24が以前にコンテンツ・サーバ22から取得した認証書(即ち、(CERT(PU-LS)S(PR-CS)))、

更に、図3に示すように、デジタル・コンテンツ12を有するパッケージ12pが次を含むことも念頭に入れ、

—このようなデジタル・コンテンツ12のコンテンツID、

KDによって暗号化されているデジタル・コンテンツ12(即ち、(KD(CONTENT)))、

—暗号化されていないライセンス取得スクリプト、および

—コンテンツ・サーバ22の秘密鍵(PR-CS)によって署名されたコンテンツ・サーバ22の公開鍵(PU-CS)を暗号化する鍵KD、

本発明の一実施形態では、鍵トランザクションの特定のシーケンスを、デジタル・コンテンツ12のライセンス16の特定の1つに関して実行する。このシーケンスは次の通りである。

【0102】

1. ライセンス16からの(PU-BB(KD))に基づいて、ユーザの計算機14上のDRMシステム32のブラック・ボックス30はその秘密鍵(PR-BB)を適用し、(KD)を取得する(ステップ1001)。(PR-BB(PU-BB(PU-BB(KD)))=(KD))。尚、重要なことは、ブラック・ボックス30は、これ以上の面倒なく、KDを用いてデジタル・コンテンツ12を解読しようとすることも可能であることを注記しておく。このような信頼は、このようなライセンス・サーバ24が、このようなブラック・ボックス30の信ぴょう性を保証する、証明機関からの認証書に基づいて、ライセンス16を発行したときに確立されている。したがって、最終ステップではなく最初のステップ

としてブラック・ボックス30が解読鍵(KD)を取得しても、DRMシステム32は、以下に説明するように、全てのライセンス16の妥当性検査および評価機能を実行し続ける。

【0103】

2. デジタル・コンテンツ12からの(KD(PU-CS))S(PR-CS))に基づいて、ブラック・ボックス30は新たに取得した解読鍵(KD)を適用して(PU-CS)を取得する(ステップ1003)。(KD(KD(PU-CS))=(PU-CS))。加えて、ブラック・ボックス30は、署名(S(PR-CS))に対して(PU-CS)を適用し、このような署名およびこのようなデジタル・コンテンツ12/パッケージ12pが有効であることを納得する(ステップ1005)。有効でない場合、プロセスを中断し、デジタル・コンテンツ12へのアクセスを拒否する。

【0104】

3. ライセンス16からの(CERT(PU-LS))S(PR-CS))に基づいて、ブラック・ボックス30は、新たに取得したコンテンツ・サーバ22の公開鍵(PU-CS)を適用し、認証書が有効であることを納得する(ステップ1007)。これは、ライセンス16を発行したライセンス・サーバ24がコンテンツ・サーバ22からの機関(authority)にそうさせ、次いで認証書の内容を検査して(PU-LS)を取得することを意味する(ステップ1009)。有効でない場合、プロセスを中止し、ライセンス16に基づくデジタル・コンテンツ12へのアクセスを拒否する。

【0105】

4. ライセンス16からの(S(PR-LS))に基づいて、ブラック・ボックス30は、新たに取得したライセンス・サーバ24の公開鍵(PR-LS)を適用して、ライセンス16が有効であることを納得する(ステップ1011)。有効でない場合、プロセスを中止し、ライセンス16に基づくデジタル・コンテンツ12へのアクセスを拒否する。

【0106】

5. 全ての妥当性検査ステップが成功し、ライセンス16内のDRL48が実

際に解読鍵(KD)で暗号化されていると仮定すると、ライセンス評価部36は、既に取得してある解読鍵(KD)を、ライセンス16から取得した(KD(DRL))に適用し、ライセンス16からライセンス条件を得る(即ちDRL48)(ステップ1013)。勿論、ライセンス16におけるDRL48が実際に解読鍵(KD)で暗号化されていない場合、ステップ1013を省略してもよい。次に、ライセンス評価部36は、DRL48を評価し、問い合わせを行い、ユーザの計算機14がライセンス16内のDRL48に基づいて、求められた態様で対応するデジタル・コンテンツ12をレンダリングする権利を有するか否か(即ち、DRL48が授権付与しているか否か)判定を行なう(ステップ1015)。ライセンス評価部36が、このような権利が存在しないと判定した場合、プロセスを中止し、ライセンス16に基づくデジタル・コンテンツ12へのアクセスを拒否する。

【0107】

6. 最後に、ライセンス16の評価の結果、ユーザの計算機14はDRL48の条件に基づいて、求められた態様で対応するデジタル・コンテンツ12をレンダリングする権利を有するという肯定的な判断が得られたと仮定すると、ライセンス評価部36は、ブラック・ボックス30が解読鍵(KD)にしたがって対応するデジタル・コンテンツ12をレンダリングできることを、このようなブラック・ボックス30に通知する。その後、ブラック・ボックス30は解読鍵(KD)を適用し、パッケージ12pからのデジタル・コンテンツ12を解読する(即ち、 $(KD(KD(CONTENT))) = (CONTENT)$)(ステップ1017)。

【0108】

先に具体化した一連のステップは、ライセンス16およびデジタル・コンテンツ12間の交互動作即ち「ピンポン動作」を表わすことを注記するのは重要である。このようなピンポン動作によって、デジタル・コンテンツ12を緊密にライセンス16に結び付けることを保証し、デジタル・コンテンツ12およびライセンス16双方が適性に発行され有効な形態で存在する場合にのみ、妥当性検査および評価プロセスを行なうことができることを保証する。加えて、ライセンス1

6からのコンテンツ・サーバ22の公開鍵(PU-C S)、および解読した形態でパッケージ12pからデジタル・コンテンツ12を得るには(そして、恐らく、解読した形態でライセンス16からライセンス条件(DRL48)を得るためにも)同じ解読鍵(KD)が必要であるので、このような項目も緊密に結び付けられる。また、署名の妥当性検査によっても、デジタル・コンテンツ12およびライセンス16が、それぞれコンテンツ・サーバ22およびライセンス・サーバ24から発行された同じ形態であることを保証する。したがって、ライセンス・サーバ24を迂回することによってデジタル・コンテンツ12を解読することは、不可能ではないにしても困難であり、デジタル・コンテンツ12またはライセンス16を変更しそして解読することも、不可能ではないにしても困難である。

【0109】

本発明の一実施形態では、署名の妥当性検査、特にライセンス16の署名の妥当性検査は、代わりに次のように行われる。図8に示すように、ライセンス・サーバ16の秘密鍵(PR-L S)によって署名を暗号化するのではなく、各ライセンス16の署名を、秘密ルート鍵(PR-R) (図示せず)によって暗号化する。この場合、各DRMシステム32のブラック・ボックス30は、秘密ルート鍵(PR-R)に対応する公開ルート鍵(PU-P) (これも図示せず)を含む。秘密ルート鍵(PR-R)は、ルート・エンティティだけがわかっており、ライセンス・サーバ24は、このようなライセンス・サーバ24がルート・エンティティを用いてライセンス16を発行するように調整した場合にのみ、ライセンス16を発行することができる。

【0110】

即ち、このような実施形態では、

1. ライセンス・サーバ24がその公開鍵(PR-L S)をルート・エンティティに供給する。

【0111】

2. ルート・エンティティはこのようなライセンス・サーバ24に、秘密ルート鍵(PR-R)によって暗号化されたライセンス・サーバ公開鍵(PU-L S)を戻す(即ち、(CERT(PU-L S) S(PR-R)))。

【0112】

3. 次に、ライセンス・サーバ24は、ライセンス・サーバの公開鍵（S（P-R-L S））によって暗号化された署名を有するライセンス16を発行し、更に、ルート・エンティティからの認証書をライセンスに添付する（CERT（P-U-L S）S（P-R-R））。

【0113】

DRMシステム18がこのように発行されたライセンス17の妥当性を検査するために、DRMシステム18は、

1. 公開ルート鍵（P-U-R）を、添付した認証書（CERT（P-U-L S）S（P-R-R））に適用し、ライセンス・サーバ公開鍵（P-U-L S）を取得し、
2. 取得したライセンス・サーバ公開鍵（P-U-L S）をライセンス16の署名（P-R-L S）に適用する。

【0114】

重要なこととして、ルート・エンティティが認証書（CERT（P-U-L S）S（P-R-R））をライセンス・サーバ24に供給することによって、このようなライセンス・サーバ24にライセンス16を発行する許可を与えるのと丁度同じように、このようなライセンス・サーバ24は同様に認証書を第2のライセンス・サーバ24に供給し（即ち、（CERT（P-U-L S 2）S（P-R-L S 1）））、これによって第2のライセンス・サーバにもライセンス16を発行させることができることも認められてしかるべきである。今や明白であろうが、第2ライセンス・サーバが発行するライセンス16は、第1認証書（CERT（P-U-L S 1）S（P-R-R））および第2認証書（CERT（P-U-L S 2）S（P-R-L S 1））を含む。同様に、このようなライセンス16は、第1および第2認証書のチェーンに従うことによって、有効性を認められる。勿論、チェーンの中に追加のリンクを加え、これらを通過するようにしてもよい。

【0115】

前述の署名妥当性検査プロセスの利点の1つとして、ルート・エンティティが定期的に秘密ルート鍵（R-P-R）を変更することによって、同様に定期的に各

ライセンス・サーバ24に新たな認証書(CERT(PU-LS)S(PR-R))を取得させることができる点にある。重要なことは、このような新たな認証書を取得する要件として、各ライセンス・サーバがそれ自体をアップグレードする必要があるということである。ブラック・ボックス30の場合と同様、ライセンス・サーバ24が比較的新しい場合、即ち、比較的最近アップグレードされている場合、ライセンス・サーバ24を攻撃して成功する可能性は低くなる。したがって、信頼の問題として、各ライセンス・サーバ24は、署名妥当性検査プロセスのような適切なアップグレード推進機構を通じて定期的にアップグレードしなければならないようにすることが好ましい。勿論、他のアップグレード機構を採用することもでき、本発明の精神および範囲から逸脱することにはならない。

【0116】

勿論、秘密ルート鍵(PR-R)を変更する場合、各DRMシステム18における公開ルート鍵(PU-R)も変更しなければならない。このような変更は、例えば、通常のブラック・ボックス30のアップグレードの間に行なえばよく、あるいは実際にはブラック・ボックス30のアップグレードを行なうことが必要となる場合もある。変更した公開ルート鍵(PU-R)は潜在的に、古い秘密ルート鍵(PR-R)に基づいて発行した古いライセンス16に対する署名の妥当性検査と干渉する可能性もあるが、このような干渉は、アップグレードしたブラック・ボックス30が古い公開ルート鍵(PU-R)全てを記憶しておくことを要求することによって、最少に抑えることができる。あるいは、このような干渉を最少に抑えるには、ライセンス16に対する署名の検証を1回だけ行なえばよいようにしてもよい。例えば、DRMシステム18のライセンス評価部36によって、最初にこのようなライセンス16を評価する。このような場合、署名の検証が行われたか否かに関する状態情報をコンパイルし、このような状態情報をDRMシステム18の状態ストア40に格納するべきであろう。

デジタル権利ライセンス48

本発明では、ライセンス評価部36は、ライセンス16の権利記述即ち条件としてデジタル権利ライセンス(DRL)48を評価し、このようなDRL48が、求められた態様でデジタル・コンテンツ12の対応する1片のレンダリングを

許可するか否か判定を行なう。本発明の一実施形態では、いずれかのDRL言語によって、ライセンス（即ち、コンテンツ所有者）がDRL48を書くことができる。

【0117】

当然理解されようが、DRL48を指定するには多くの方法がある。したがって、いずれのDRL言語においても、高い柔軟性を許容しなければならない。しかしながら、特定のライセンス言語でDRL48の全ての面を指定することは非実用的であり、このような言語の著者が、個々のデジタル・ライセンスが望むライセンスの可能な態様全てを確認できるようにすることは可能性が非常に低い。更に、非常に洗練されたライセンス言語は不要の場合もあり、比較的単純なDRL48を与えるライセンスにとっては障害となる場合もある。しかしながら、DRL48をどのように指定するかについてライセンスを不必要に制約してはならない。同時に、ライセンス評価部36は、常に多数の具体的なライセンスに関する問題に対して、DRL48から回答を得ることができなければならない。

【0118】

ここで図11を参照すると、本発明では、DRL48はいずれのライセンス言語でも指定することができるが、言語識別子即ちタグ54を含む。ライセンス評価部36は、ライセンス16を評価し、次いで言語タグ54を調べる暫定ステップを実行し、このような言語を識別し、次いで適切なライセンス言語エンジン52を選択し、このように識別した言語のライセンス16にアクセスする。当然理解されようが、このようなライセンス言語エンジン52が存在し、ライセンス評価部36にアクセス可能でなければならない。存在しない場合、言語タグ54および／またはDRL48は、このような言語エンジン52を取得する場所56（典型的にウェブ・サイト）を含むことが好ましい。

【0119】

典型的に、言語エンジン52は、ハード・ドライブのような、ユーザの計算機14のメモリに常駐する、実行可能ファイルまたは1組のファイルという形態を取る。言語エンジン52は、ライセンス評価部36がDRL48に直接問い合わせを行なう際に補助し、ライセンス評価部36は、仲介役として作用する言語エ

ンジン48等を介して間接的にDRL48に問い合わせを行なう。言語エンジン52を実行すると、RAMのような、ユーザの計算機14のメモリのワーク・スペースにおいて走る。しかしながら、言語エンジン52はその他のいずれの形態でも用いることができ、本発明の精神および範囲から逸脱することはない。

【0120】

好ましくは、いずれの言語エンジン52およびいずれのDRL言語も、ライセンス評価部36が、DRL48によって回答されることを期待する、少なくともある数の具体的なライセンスに関する質問に対応するようにする。したがって、ライセンス評価部36は、いずれの特定のDRL言語にも結び付けられていない。DRL48はいずれの適切なDRL言語でも書くことができ、新たなライセンス言語で指定されたDRL48は、既存のライセンス評価部36に、対応する新たな言語エンジン52を取得させることによって、このようなライセンス評価部36が採用することができる。

DRL言語

DRL言語の例を2つ、それぞれのDRL48に具体化した場合について、以下に示す。最初の「簡単な」DRL48は、ライセンス属性を指定するDRL言語で書かれており、一方2番目の「スクリプト」DRL48は、DRL48に指定されているスクリプトにしたがって機能を実行することができるDRL言語で書かれている。DRL言語で書かれている場合、各コード行の意味は、その言語規則 (linguistics) および／または以下に続く属性の記述チャートに基づいて明らかにはずである。

単純なDRL48

【0121】

【表1】

Simple DRL 48:

<LICENSE>

<DATA>

<NAME>Beastie Boy's Play</NAME>

<ID>39384</ID>

<DESCRIPTION>Play the song 3 times</DESCRIPTION>

<TERMS></TERMS>

<VALIDITY>

<NOTBEFORE>19980102 23:20:14Z</NOTBEFORE>

<NOTAFTER>19980102 23:20:14Z</NOTAFTER>

</VALIDITY>

<ISSUEDDATE>19980102 23:20:14Z</ISSUEDDATE>

<LICENSORSITE>http://www.foo.com</LICENSORSITE>

```

<CONTENT>
  <NAME>Beastie Boy's</NAME>
  <ID>392</ID>
  <KEYID>39292</KEYID>
  <TYPE>MS Encrypted ASF 2.0</TTYPE>
</CONTENT>
<OWNER>
  <ID>939KDKD393KD</ID>
  <NAME>Universal</NAME>
  <PUBLICKEY></PUBLICKEY>
</OWNER>
<LICENSEE>
  <NAME>Arnold</NAME>
  <ID>939KDKD393KD</ID>
  <PUBLICKEY></PUBLICKEY>
</LICENSEE>
<PRINCIPAL TYPE='AND'>
  <PRINCIPAL TYPE='OR'>
    <PRINCIPAL>
      <TYPE>x86Computer</TYPE>
      <ID>3939292939d9e939</ID>
      <NAME>Personal Computer</NAME>
      <AUTHTYPE>Intel Authenticated Boot PC
      SHA-1 DSA512</AUTHTYPE>
      <AUTHDATA>29293939</AUTHDATA>
    </PRINCIPAL>
    <PRINCIPAL>
      <TYPE>Application</TYPE>
      <ID>2939495939292</ID>
      <NAME>Window's Media Player</NAME>
      <AUTHTYPE>Authenticode          SHA-
      1</AUTHTYPE>
      <AUTHDATA>93939</AUTHDATA>
    </PRINCIPAL>
  </PRINCIPAL>
</PRINCIPAL>
  <PRINCIPAL>
    <TYPE>Person</TYPE>
    <ID>39299482010</ID>
    <NAME>Arnold Blinn</NAME>
    <AUTHTYPE>Authenticate user</AUTHTYPE>
    <AUTHDATA>\\redmond\arnoldb</AUTHDATA>
  </PRINCIPAL>
</PRINCIPAL>

```

```

<DRLTYPE>Simple</DRLTYPE> [the language tag 54]
<DRLDATA>
  <START>19980102 23:20:14Z</START>
  <END>19980102 23:20:14Z</END>
  <COUNT>3</COUNT>
  <ACTION>PLAY</ACTION>
</DRLDATA>
<ENABLINGBITS>aaaabbbbccccddd</ENABLINGBITS>
</DATA>
<SIGNATURE>
<SIGNERNAME>Universal</SIGNERNAME>
  <SIGNERID>9382ABK3939DKD</SIGNERID>
  <HASHALGORITHMID>MD5</HASHALGORITHMID>
  <SIGNALGORITHMID>RSA 128</SIGNALGORITHMID>
  <SIGNATURE>xxxxxxxxxxxxxx</SIGNATURE>
  <SIGNERPUBLICKEY></SIGNERPUBLICKEY>
  <CONTENTSIGNEDSIGNERPUBLICKEY></CONTENTSIGNEDSIGNERPUBLICKEY>
</SIGNATURE>
</LICENSE>

```

【0122】

【表2】

Script DRL 48:

```

<LICENSE>
  <DATA>
    <NAME>Beastie Boy's Play</NAME>
    <ID>39384</ID>
    <DESCRIPTION>Play the song unlimited</DESCRIPTION>
    <TERMS></TERMS>
    <VALIDITY>
      <NOTBEFORE>19980102 23:20:14Z</NOTBEFORE>
      <NOTAFTER>19980102 23:20:14Z</NOTAFTER>
    </VALIDITY>
    <ISSUEDDATE>19980102 23:20:14Z</ISSUEDDATE>
    <LICENSORSITE>http://www.foo.com</LICENSORSITE>
    <CONTENT>
      <NAME>Beastie Boy's</NAME>
      <ID>392</ID>
      <KEYID>39292</KEYID>
      <TYPE>MS Encrypted ASF 2.0</TYPE>
    </CONTENT>
    <OWNER>
      <ID>939KDKD393KD</ID>
    </OWNER>
  </DATA>
</LICENSE>

```

```

<NAME>Universal</NAME>
<PUBLICKEY></PUBLICKEY>
</OWNER>
<LICENSEE>
  <NAME>Arnold</NAME>
  <ID>939KDKD393KD</ID>
  <PUBLICKEY></PUBLICKEY>
</LICENSEE>
<DRLTYPE>Script</DRLTYPE> [the language tag 54]
<DRLDATA>
  function on_enable(action, args) as boolean
    result = False
    if action = "PLAY" then
      result = True
    end if
    on_action = False
  end function
  ...
</DRLDATA>
</DATA>
<SIGNATURE>
  <SIGNERNAME>Universal</SIGNERNAME>
  <SIGNERID>9382</SIGNERID>
  <SIGNERPUBKEY></SIGNERPUBKEY>
  <HASHID>MD5</HASHID>
  <SIGNID>RSA 128</SIGNID>
  <SIGNATURE>xxxxxxxxxxxxxxxx</SIGNATURE>
  <CONTENTSIGNEDSIGNERPUBKEY></CONTENTSIGNEDSIGNERPUBKEY>
</SIGNATURE>
</LICENSE>

```

以上に指定した2つのDRLにおいて、掲示した属性は、以下の記述およびデータ・タイプを有する。

【0123】

【表3】

属性	説明	データ・タイプ
I d	ライセンスの I D	G U I D
名称	ライセンスの名称	ストリング
コンテンツ I d	コンテンツの I D	G U I D
コンテンツ鍵 I d	コンテンツの暗号化鍵の I D	G U I D
コンテンツ名	コンテンツの名称	ストリング
コンテンツ・タイプ	コンテンツのタイプ	ストリング
所有者 I d	コンテンツの所有者の I D	G U I D
所有者名	コンテンツの所有者の名称	ストリング
所有者公開鍵	コンテンツ所有者の公開鍵。これは、コンテンツ所有者のベース-64エンコード公開鍵である	ストリング
ライセンシ I d	ライセンスを得る人の I d。ヌルでもよい。	G U I D
ライセンシ名	ライセンスを得る人の名前。ヌルでもよい。	ストリング
ライセンシ公開鍵	ライセンシの公開鍵これは、ライセンシのベース-64エンコード公開鍵である。ヌルでもよい。	ストリング
説明	人が読める単純なランセンスの説明	ストリング
条件	ライセンスの法的条件。これは法的文書 (prose) を含むページへのポインタとすることもできる。	ストリング
有効性終了	ライセンス有効期間終了	日付
有効性発生	ライセンスの有効期間開始	日付
発行日	ライセンスを発行した日付	日付
D R L タイプ	D R L の タイプ 。 例は、"SIMPLE"または"SCRIPT"を含む。	ストリング
D R L データ	D R L に特定なデータ	ストリング
許可ビット	これらのビットは、実際のコンテンツへのアクセスを許可するビットである。これらのビットの解釈は、アプリケーションに委ねられるが、典型的に、これはコンテンツ解読のための秘密鍵である。このデータはベース-64エンコードされて	ストリング

	いる。これらのビットは、個々の機械の公開鍵を用いて暗号化されていることを注記しておく。	
署名者 I d	ライセンスに署名した人の I D	G U I D
署名者名	ライセンスに署名した人の名前	ストリング
署名者公開鍵	ライセンスに署名した人の公開鍵。これは、署名者のベース-64エンコード公開鍵である。	ストリング
コンテンツ署名署名者公開鍵	コンテンツ・サーバの秘密鍵によって署名されたライセンスに署名した人の公開鍵。この署名を検証する公開鍵は、コンテンツに暗号化されている。これは、ベース-64エンコードされている。	ストリング
ハッシュ A l g I d	ハッシュを生成するために用いるアルゴリズム。これは、"MD5"のようなストリングである。	ストリング
署名 A l g I d	署名を生成するために用いるアルゴリズム。これは、"RSA128"のようなストリングである。	ストリング
署名	データの署名。これはベース-64エンコード・データである。	ストリング

メソッド

先に論じたように、言語エンジン52およびいずれのDRL言語も、DRL48が回答することをデジタル・ライセンス評価部36が期待する、少なくともある数の特定のライセンスに関する質問に対応することが好ましい。このような対応する質問を認識することは、本発明の精神および範囲から逸脱することなく、あらゆる質問を含むことができ、先にあげた2つのDRL48の例において用いられる用語と一致し、本発明の一実施形態では、このような対応する質問または、以下のような、「メソッド」は「アクセス・メソッド」、「DRLメソッド」、および「使用許可メソッド」を含む。

アクセス・メソッド

アクセス・メソッドは、最上位の属性に対してDRL 48に問い合わせるために用いる

VARIANT QueryAttribute (BSTR鍵)

有効な鍵は、各々BSTRバリエーションを戻す、Licence.Name, License.Id, Content.Name, Content.Id, Content.Type, Owner.Name, Owner.Id, Owner.PublicKey, Licensee.Name, Licensee.Id, Licensee.PublicKey, Description, およびTerms、ならびに、各々Dateバリエーションを戻すValidity.StartおよびValidity.Endを戻す。

DRLメソッド

以下のDRLメソッドの実装は、各DRL 48毎に異なる。DRLメソッドの多くは、'data'と称するバリエーション・パラメータを含み、DRL 48と一層進んだ情報を交信することを目的とする。これは主に今後の拡張性のためにある。

Boolean IsActivated (バリエーション・データ)

このメソッドは、DRL 48/ライセンス16が活性化しているか否かを示すブール変数を戻す。活性化したライセンス16の一例は、限定動作ライセンス16であり、最初の再生のときに48時間だけアクティブとなる。

Activate (バリエーション・データ)

このメソッドは、ライセンス16を活性化するために用いられる。一旦ライセンス16が活性化されると、不活性化することはできない。

Variant QueryDRL (バリエーション・データ)

このメソッドは、一層進んだDRL 48と通信するために用いられる。これは、主にDRL 48の特徴集合の今後の拡張性に関する。

Variant GetExpires (BSTRアクション、バリエーション・データ)

このメソッドは、投入したアクションに関するライセンス16の満期日を戻す。戻り値がNULLの場合、ライセンスは無期限であると見なされるか、または未だ活性化されていない等のために、未だ満期日を有していない。

Variant GetCount (BSTRアクション、バリエーション・データ)

このメソッドは、投入されたアクションの残り動作回数を戻す。NULLが戻

された場合、動作は無限回数実行することができる。

Boolean IsEnabled (BSTRアクション、バリエント・データ)

このメソッドは、ライセンス16が、現時点において要求されているアクションに対応するか否かについて示す。

Boolean IsSunk (BSTRアクション、バリエント・データ)

このメソッドは、ライセンス16に対して支払が行われたか否かについて示す。前金で支払が済んでいるライセンス16はTRUEを返し、一方使用時に料金を徴収するライセンス16のように、前金で支払が済んでいないライセンス16は、FALSEを返す。

【0124】

使用許可メソッド

これらのメソッドは、コンテンツを解読する際に用いるライセンス16を許可するために用いられる。

Boolean Validate (BSTR鍵)

このメソッドはライセンス16の妥当性を検査するために用いられる。終了した鍵は、ライセンス16の署名の妥当性検査に用いる、対応のデジタル・コンテンツ12の解読鍵(KD)(即ち、(KD(PU-BB)))によって暗号化された、ブラック・ボックス30の公開鍵(PU-BB)である。戻り値がTRUEである場合、ライセンス16が有効であることを示す。戻り値がFALSEである場合無効を示す。

int OpenLicense 16 (BSTRアクション、BSTR鍵、バリエント・データ)

このメソッドは、解読した許可ビットにアクセスする準備のために用いられる。終了した鍵は、前述のように、(KD(PU-BB))である。戻り値が0の場合、成功を示す。他の戻り値を定義することができる。

BSTR GetDecryptedEnablingBits (BSTRアクション、バリエント・データ)

Variant GetDecryptedEnablingBitsAsBinary (BSTRアクション、バリエント・データ)

これらのメソッドは、解読した形態の許可ビットにアクセスするために用いられる。これが多数の理由のいずれかのために成功しなかった場合、ヌル・ストリ

ングまたはヌル・バリエントが戻される。

void CloseLicense 16 (BSTRアクション、バリエント・データ)

このメソッドは、終了したアクションを実行するために、許可ビットへのアクセスを解除するために用いられる。これが多数の理由のいずれかのために成功しなかった場合、ヌル・ストリングが戻される。

発見法

先に論じたように、同じ1片のデジタル・コンテンツ12に対して多数のライセンス16が存在する場合、ライセンス16の1つを選択して用いなければならない。前述のメソッドを用いると、以下の発見法を実施してこのような選択を行なうことができる。即ち、1片のデジタル・コンテンツ12に対してあるアクション(例えば、「再生」)を実行するためには、以下のステップを実行することができる。

【0125】

1. 特定の1片のデジタル・コンテンツ12に適用するライセンス16全てを得る。

2. このようなライセンス16に対してIsEnabled関数をコールすることによってアクションをイネーブルしない各ライセンス16を削除する。

【0126】

3. このようなライセンス16に対してIsActiveをコールすることによってアクティブでない各ライセンス16を削除する。

4. このようなライセンス16に対してIsSunkをコールすることによって、前金で支払が済んでいない各ライセンスを削除する。

【0127】

5. いずれかのライセンス16が残されている場合、これを用いる。再生回数制限ライセンス16を用いる前に、特に再生回数無制限ライセンス16に満期日がある場合、再生回数無制限ライセンスを用いる。いずれの時点においても、ユーザは、例え選択が価格効率的でなくとも、既に取得してある特定のライセンス16を選択することが許されて当然である。したがって、ユーザは、恐らくDRMシステム32には明白でない判断基準に基づいて、ライセンス16を選択

することができる。

【0128】

6. 放置されているライセンス16がある場合、それを示すステータスを戻す。すると、ユーザには、
使用可能であれば、前金で支払が済んでいないライセンス16を用いる、
使用可能であれば、ライセンス16を活性化する、および／または
ライセンス・サーバ24からライセンス取得を実行する、
という選択肢が与えられる。

結論

本発明に関連して実行するプロセスを達成するために必要なプログラミングは、比較的単純であり、関連のあるプログラミング分野の人々には明白であるはずである。したがって、このようなプログラミングをここには添付しない。つまり、本発明を達成するためには、本発明の精神および範囲から逸脱することなく、いずれの特定のプログラミングでも用いることができる。

【0129】

前述の説明では、本発明は、新規でかつ有用な実施アーキテクチャ10から成り、デジタル・コンテンツ12を制御し任意の形態でレンダリングまたは再生することを可能とし、このような制御は柔軟性があり、このようなデジタル・コンテンツ12のコンテンツ所有者によって定義可能であることがわかる。また、本発明は、デジタル・コンテンツ12が、たとえコンテンツ所有者の制御の下にない計算機14上でレンダリングするにしても、コンテンツ所有者による指定通りにしかデジタル・コンテンツ12をレンダリングしない、新規で有用なレンダリング環境の制御から成る。更に、本発明は、コンテンツ所有者が許可しない方法で、このような計算機14のユーザが1片のデジタル・コンテンツ12にアクセスしようとする試みに対してでさえ、このようなデジタル・コンテンツ12に関して、このような計算機14上でコンテンツ所有者の権利を実施する信頼コンピュータネットワークから成る。

【0130】

尚、本発明の概念から逸脱することなく、上述の実施形態には変更も可能であ

ることは認められよう。したがって、本発明は、開示した特定の実施形態に限定されるのではなく、添付した特許請求の範囲によって規定される本発明の精神および範囲内の変更も包含することを意図することは理解されよう。

【図面の簡単な説明】

【図1】

本発明の一実施形態による実施アーキテクチャを示すブロック図である。

【図2】

本発明の一実施形態による図1のアーキテクチャのオーサリング・ツールのブロック図である。

【図3】

本発明の一実施形態による図1のアーキテクチャと共に用いるデジタル・コンテンツを有するデジタル・コンテンツ・パッケージのブロック図である。

【図4】

本発明の一実施形態による図1のユーザの計算機のブロック図である。

【図5】

図5Aは本発明の一実施形態にしたがってコンテンツをレンダリングするための、図4の計算機のデジタル権利管理(DRM)システムと共に実行するステップを示すフロー図である。

図5Bは本発明の一実施形態にしたがってコンテンツをレンダリングするための、図4の計算機のデジタル権利管理(DRM)システムと共に実行するステップを示すフロー図である。

【図6】

本発明の一実施形態にしたがって、何らかの有効な権限付与ライセンスがあるか否か判定するために、図4のDRMシステムと共に実行するステップを示すフロー図である。

【図7】

本発明の一実施形態にしたがってライセンスを取得するために、図4のDRMシステムと共に実行するステップを示すフロー図である。

【図8】

本発明の一実施形態にしたがって図1のアーキテクチャと共に用いるデジタル使用許諾のブロック図である。

【図9】

本発明の一実施形態にしたがって新たなブラック・ボックスを取得するために、図4のDRMシステムと共に実行するステップを示すフロー図である。

【図10】

本発明の一実施形態にしたがってライセンスおよび1片のデジタル・コンテンツの妥当性を検査し、コンテンツをレンダリングするために、図4のDRMシステムと共に実行する鍵トランザクション・ステップを示すフロー図である。

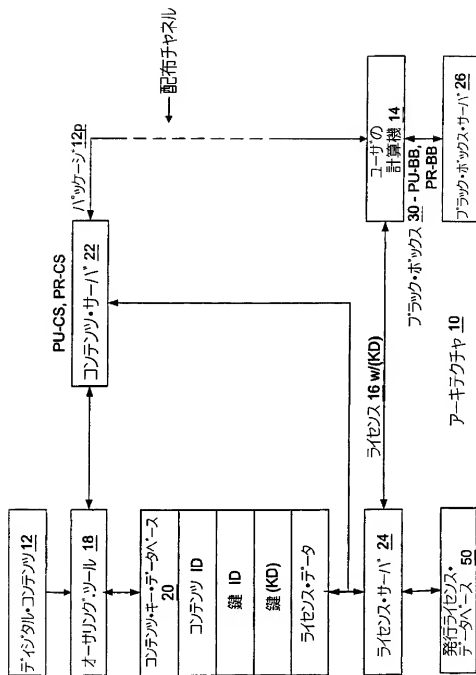
【図11】

本発明の一実施形態によるライセンスのデジタル権利ライセンス(DRL)、およびDRMを解釈する言語エンジンと共に、図4のライセンス評価部を示すブロック図である。

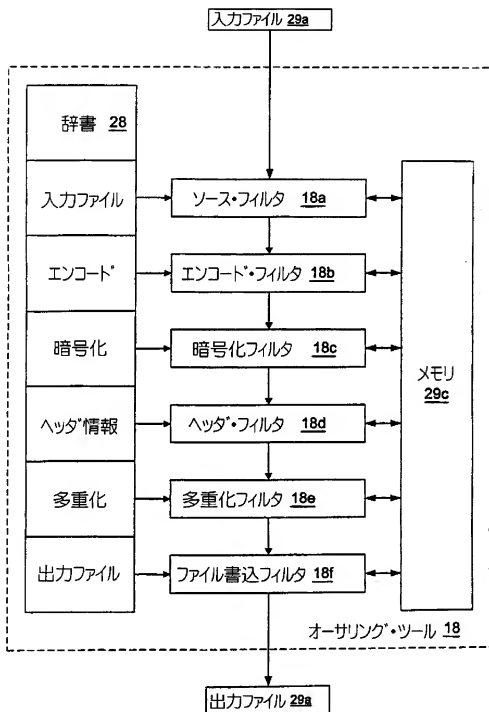
【図12】

本発明の態様および／またはその一部を組み込むことができる汎用コンピュータ・システムを表わすブロック図である。

【図1】



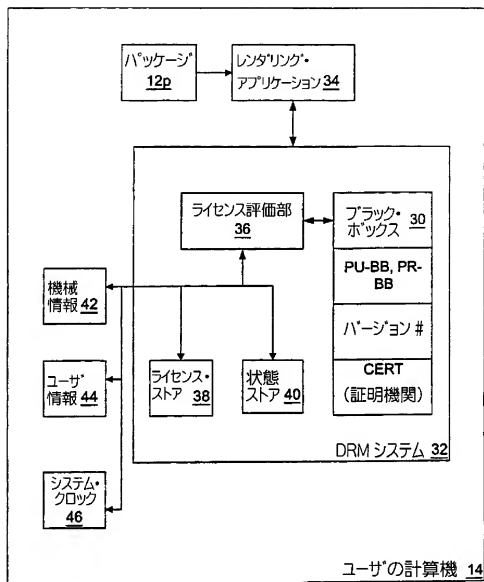
【図2】



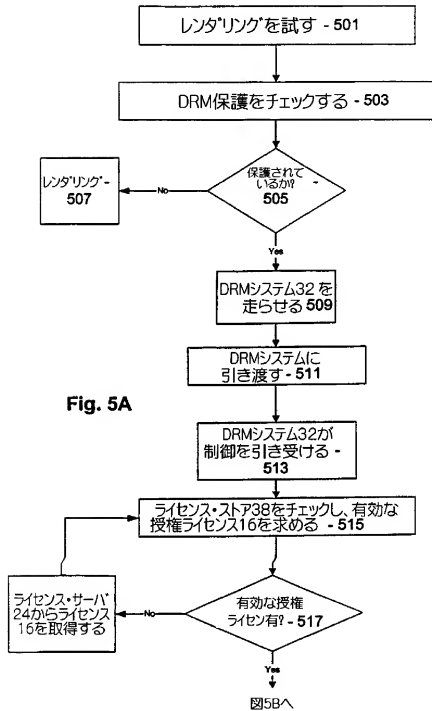
【図3】

デジタル・コンテンツ・パッケージ <u>12p</u>
KD (デジタル・コンテンツ <u>12</u>)
コンテンツ ID
鍵 ID
ライセンス取得情報
KD (PU-CS) S (PR-CS)

【図4】



【図5A】



【図5B】

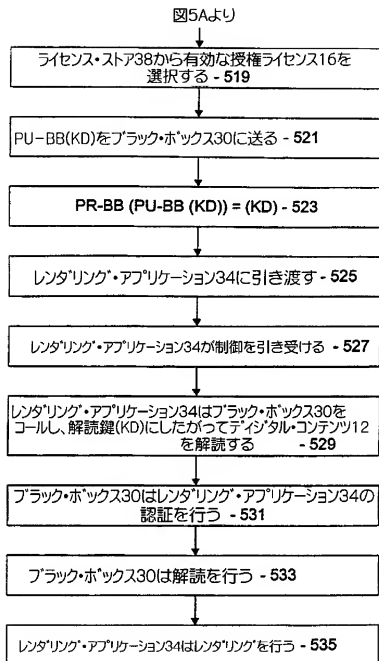
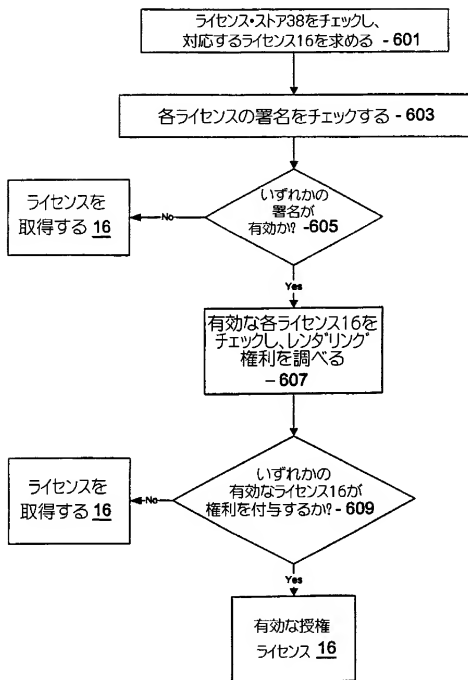
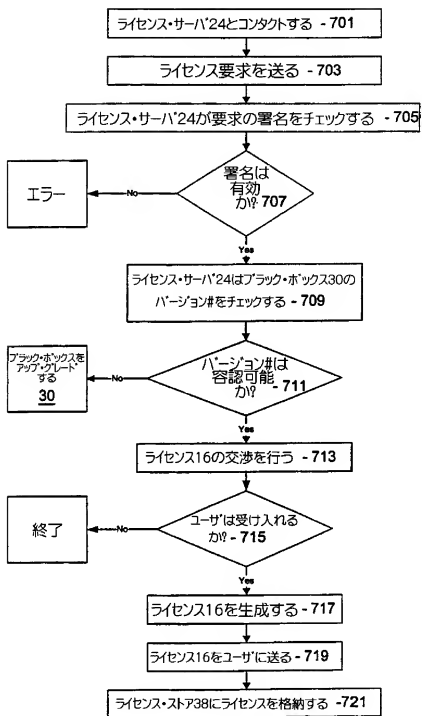


Fig. 5B

【図6】



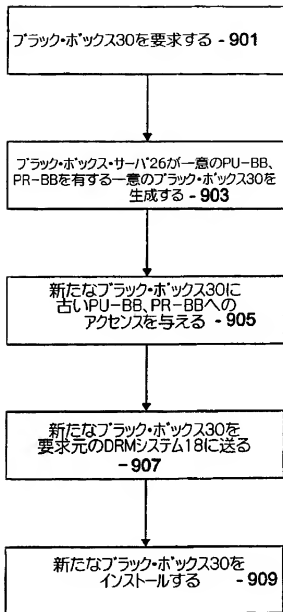
【図7】



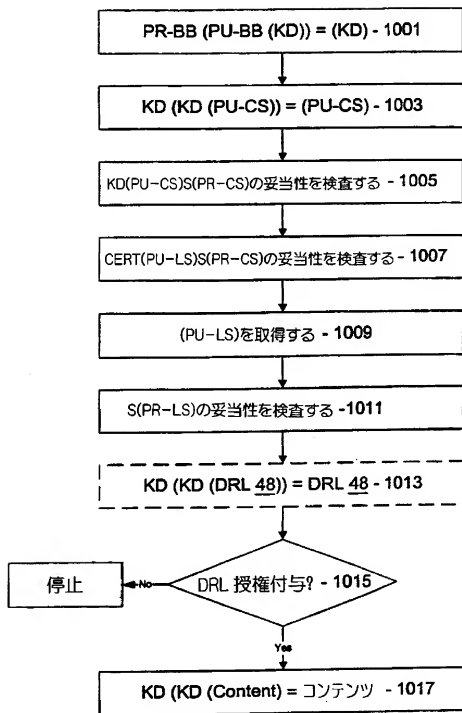
【図8】

ライセンス <u>16</u>
コンテンツ ID
DRL <u>48</u> or KD (DRL <u>48</u>)
PU-BB (KD)
S (PR-LS)
CERT (PU-LS) S (PR-CS)

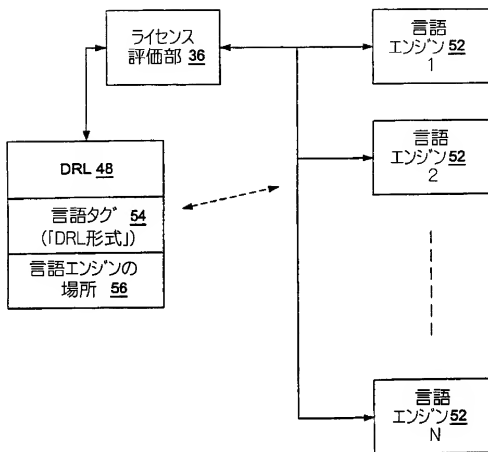
【図9】



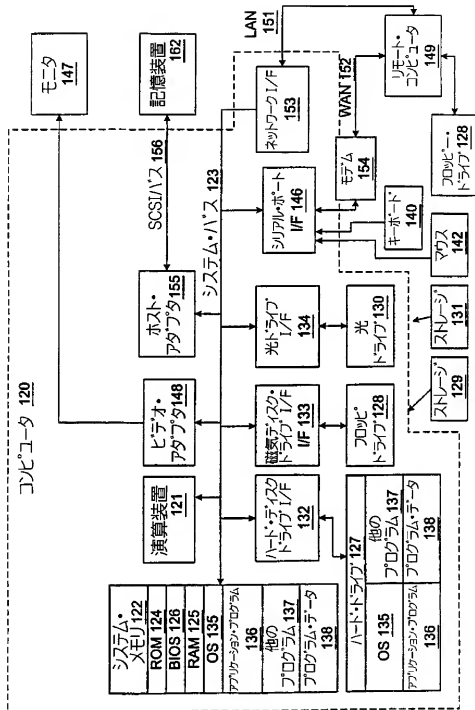
【図10】



【図11】



【図12】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	FI	テーマコード(参考)
		H04L 9/00	G01E
(81)指定国	EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW		
(72)発明者	アブブリ, ラジャセクハー		
	アメリカ合衆国ワシントン州98039, メディナ, ノースイースト・テニス・ストリート 7844		
(72)発明者	ブリン, アーノルド・エヌ		
	アメリカ合衆国ワシントン州98004, ベルビュー, ノースイースト・トゥエンティセヴンス・ストリート 9401		
(72)発明者	ジョーンズ, トーマス・シー		
	アメリカ合衆国ワシントン州98053-3618, レッドモンド, ノースイースト・シックス・ストリート 23617		
(72)発明者	マンファードリ, ジョン・エル		
	アメリカ合衆国ワシントン州98053, レッドモンド, トウハンドレッドアンドフォーティファイブ・ウェイ・ノースイースト 7921		
(72)発明者	ベル, ジェフリー・アール・シー		
	アメリカ合衆国ワシントン州98013, シアトル, ノース・シックスティセヴンス・ストリート 107		
(72)発明者	ヴェンカテサン, ラマランスナム		
	アメリカ合衆国ワシントン州98052, レッドモンド, ノースイースト・トゥエンティセカンド・コート 17208		
(72)発明者	イングラント, ボール		
	アメリカ合衆国ワシントン州98008, ベルビュー, ノースアップ・ウェイ 16659		

(72)発明者 ジャクボウスキ, マリウス・エイチ
 アメリカ合衆国ワシントン州98007, ペル
 ビュー, ノースイースト・シックスティー
 ン・ブレイス 15212, ナンバー 28

(72)発明者 ユ, ハイ・イン・ヴィンセント
 アメリカ合衆国ワシントン州98007, ペル
 ビュー, リンハンドレッドフォーティフ
 ース・アベニュー・ノースイースト 809,
 ナンバー シー 4

F ターム(参考) 5B085 AA08 BG04 BG07
 5J104 AA16 EA04 EA15 MA01 MA05
 NA02 PA07